Probabilistic Algorithm for Polynomial Optimization over a Real Algebraic Set

Aurélien Greuet, Mohab Safey El Din

PROBABILISTIC ALGORITHM FOR POLYNOMIAL OPTIMIZATION OVER A REAL ALGEBRAIC SET

AURÉLIEN GREUET * † ‡ § AND MOHAB SAFEY EL DIN † §

Abstract. Let $f, f_1, \ldots, f_s$ be n-variate polynomials with rational coefficients of maximum degree D and let V be the set of common complex solutions of $\mathbf{F} = (f_1, \ldots, f_s)$. We give an algorithm which, up to some regularity assumptions on $\mathbf{F}$, computes an *exact* representation of the global infimum $f^\star$ of the restriction of the map $x \to f(x)$ to $V \cap \mathbb{R}^n$, i.e. a univariate polynomial vanishing at $f^\star$ and an isolating interval for $f^\star$. Furthermore, it decides whether $f^\star$ is reached and if so, it returns $x^\star \in V \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$.

This algorithm is *probabilistic*. It makes use of the notion of polar varieties. Its complexity is essentially *cubic* in $(sD)^n$ and linear in the complexity of evaluating the input. This fits within the best known *deterministic* complexity class $D^{O(n)}$.

We report on some practical experiments of a first implementation that is available as a MAPLE package. It appears that it can tackle global optimization problems that were unreachable by previous exact algorithms and can manage instances that are hard to solve with purely numeric techniques. As far as we know, even under the extra genericity assumptions on the input, it is the first probabilistic algorithm that combines practical efficiency with good control of complexity for this problem.

Key words. Global optimization, polynomial optimization, polynomial system solving, real solutions

AMS subject classifications.
90C26 Nonconvex programming, global optimization.
13P25 Applications of commutative algebra (e.g., to statistics, control theory, optimization, etc.).
14Q20 Effectivity, complexity.
68W30 Symbolic computation and algebraic computation.
68W05 Nonnumerical algorithms.
13P15 Solving polynomial systems; resultants.

1. Introduction.

Let $\mathbf{X} = X_1, \ldots, X_n$ be indeterminates, $f, f_1, \ldots, f_s$ be polynomials in $\mathbb{Q}[\mathbf{X}]$ of maximal degree D and $V = V(\mathbf{F})$ be the set of common complex solutions of $\mathbf{F} = (f_1, \ldots, f_s)$. We focus on the design and the implementation of *exact* algorithms for solving the polynomial optimization problem which consists in computing and exact representation of the global infimum $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. It is worth to note that, at least under some genericity assumptions, polynomial optimization problems whose constraints are non-strict inequalities can be reduced to the one with polynomial equations (see e.g. [6] and references therein).

Motivation and prior work. While polynomial optimization is well-known to be NP-hard (see e.g. [57]), it has attracted a lot of attention since it appears in various

*Laboratoire de Mathématiques (LMV-UMR8100)
Université de Versailles-Saint-Quentin
45 avenue des États-unis, 78035 Versailles Cedex, France
†Sorbonne Universités, Univ. Pierre et Marie Curie (Paris 6)
INRIA, Paris Rocquencourt Center, POLSYS Project,
LIP6/CNRS, UMR 7606,
Institut Universitaire de France,
Mohab.Safey@lip6.fr
*Université de Lille 1
Cité scientifique - bâtiment M3
59655 Villeneuve d'Ascq, France
Aurelien.Greuet@univ-lille1.fr

§Mohab Safey El Din and Aurélien Greuet are supported by the GEOLMI grant (ANR 2011 BS03 011 06) of the French National Research Agency.

areas of engineering sciences (e.g. control theory [38, 40], static analysis of programs [17, 56], computer vision [1, 2], economics, etc.). In this area, one challenge is to combine practical efficiency with reliability for polynomial optimization solvers.

One way to reach this goal is to relax the polynomial optimization problem by computing algebraic certificates of positivity proving lower bounds on $f^\star$. This is achieved with methods computing sums of squares decompositions of polynomials. In this context, one difficulty is to overcome the fact that a nonnegative polynomial is not necessarily a sum of squares. Various techniques have been studied, see e.g. [19, 33, 36, 39, 49, 59, 74]. These approaches use semi-definite programming relaxations ([60, 76]) and numerical solvers of semi-definite programs. Sometimes, a sum of squares decomposition with rational coefficients can be recovered from such a decomposition computed with floating point coefficients (see [46, 61]). Algorithms for computing sums of squares decompositions with rational coefficients have also been designed [35, 72]. Some cases of ill-conditionedness have been identified ([34]), but there is no general method to overcome them. It should also be noticed that techniques introduced to overcome situations where a non-negative polynomial is not a sum of squares rely on using gradient varieties [19, 33, 59] which are close to polar varieties introduced in the context of symbolic computation for studying real algebraic sets (see e.g. [4, 5, 7, 68]), quantifier elimination (see e.g. [42, 43]) or connectivity queries (see e.g. [70, 71]).

Another way to combine reliability and practical efficiency is to design algorithms relying on symbolic computation that solve the polynomial optimization problem. Indeed, it can be seen as a special quantifier elimination problem over the reals and a goal would be to design a dedicated algorithm whose complexity meets the best known bounds and whose practical behaviour reflects its complexity.

Quantifier elimination over the reals can be solved by the cylindrical algebraic decomposition algorithm [13]. This algorithm deals with general instances and has been studied and improved in many ways (see e.g. [11, 14, 15, 41, 55]). However, its complexity is doubly exponential in the number of variables. In practice, its best implementations are limited to non trivial problems involving 4 variables at most.

In [8], a deterministic algorithm whose complexity is singly exponential in the number of alternations of quantifiers is given. On polynomial optimization problems, this specializes to an algorithm for polynomial optimization that runs in time $D^{O(n)}$ (see [9, Chapter 14]). The techniques used to get such complexity results such as infinitesimal deformations did not provide yet practical results that reflect this complexity gain. While in some special cases, practical algorithms for one-block quantifier elimination problems have been derived by avoiding the use of infinitesimals [42, 43], the problem of obtaining fast algorithms in theory and in practice for polynomial optimization remained open.

Thus, our goal is to obtain an efficient algorithm for solving the polynomial optimization problem in theory and in practice. Thus, we expect its complexity to lie within $D^{O(n)}$ operations but with a good control on the complexity constant in the exponent. We allow to have regularity assumptions on the input that are reasonable in practice (e.g. rank conditions on the Jacobian matrix of the input equality constraints). We also allow probabilistic algorithms provided that probabilistic aspects do not depend on the input but on random choices performed when running the algorithm.

A first attempt towards this goal is in [67]. Given a n-variate polynomial f of degree D, a probabilistic algorithm computing $\inf_{x\in\mathbb{R}^n} f(x)$ in $O\left(n^7 D^{4n}\right)$ operations in

$\mathbb{Q}$ is given. Moreover, it is practically efficient and has solved problems intractable before (up to 6 variables). Our goal is to generalize this approach to the case of equality constraints and get an algorithm whose complexity is essentially cubic in $(sD)^n$ and linear in the evaluation complexity of the input.

Main results. We provide a probabilistic algorithm based on symbolic computation solving the polynomial optimization problem up to some regularity assumptions on the equality constraints whose complexity is essentially cubic in $(sD)^n$. We also provide an implementation of it and report on its practical behaviour which reflects its complexity and allows to solve problems that are either hard from the numerical point of view or unreachable by previous algorithms based on symbolic computation.

Before describing these contributions in detail, we start by stating our regularity assumptions which hold on the equality constraints. In most of applications, the Jacobian matrix of $\mathbf{F} = (f_1, \ldots, f_s)$ has maximal rank at all points of the set of common solutions of $\mathbf{F}$. In algebraic terms, this implies that this solution set is smooth of co-dimension s, complete intersection and the ideal generated by $\mathbf{F}$ (i.e. the set of algebraic relations generated by $\mathbf{F}$) is radical.

Our regularity assumptions are a bit more general than the situation we just described. In the sequel, we say that $\mathbf{F}$ satisfies assumption $\mathbf{R}$ if the following holds:

- the ideal $\langle \mathbf{F} \rangle$ is radical,
- $V(\mathbf{F})$ is equidimensional of dimension $d > 0$,
- $V(\mathbf{F})$ has finitely many singular points.

Under these assumptions, we provide an algorithm that decides the existence of $f^\star = \inf_{x \in V(\mathbf{F}) \cap \mathbb{R}^n} f(x)$ and, whenever $f^\star$ exists, it computes an exact representation of it (i.e. a univariate polynomial vanishing at $f^\star$ and an isolating interval for $f^\star$). It can also decide if $f^\star$ is reached and if this is the case it can return a minimizer $x^\star$ such that $f(x^\star) = f^\star$.

We count arithmetic operations $+, -, \times, \div$ in $\mathbb{Q}$ and sign evaluation at unit cost. We use the soft-O notation: $\widetilde{O}(a)$ indicates the omission of polylogarithmic factors in a. The complexity of the algorithm described in this paper is essentially cubic in $(sD)^n$ and linear in the complexity of evaluating f and $\mathbf{F}$. For instance if the Jacobian matrix of $\mathbf{F}$ has full rank at all points of $V(\mathbf{F})$ (this is a bit more restrictive than $\mathbf{R}$) then the algorithm performs

$$\widetilde{O}\left(L\left(\sqrt[3]{2}\,(s+1)\,D\right)^{3(n+2)}\right)$$

arithmetic operations in $\mathbb{Q}$ (see Theorem 6.10 for the general case in Section 6).

Note that this algorithm is a strict generalization of the one given in [67]. Note also that when the infimum is reached, we compute a minimizer without any assumption on the dimension of the set of minimizers.

Our algorithm follows a classical pattern which is used for quantifier elimination over the reals. It first performs a change of coordinates to ensure some technical assumptions that are satisfied in general position. Then, roughly speaking, it computes an ordered finite set of real numbers containing $f^\star$. Moreover, for any interval between two consecutive numbers in this set is either contained in $f(V(\mathbf{F}) \cap \mathbb{R}^n)$ or has an empty intersection with $f(V(\mathbf{F}) \cap \mathbb{R}^n)$.

To compute this set, we use geometric objects which are close to the notion of polar varieties which, under $\mathbf{R}$, are critical loci of some projections ; we refer to [7] for more details on several properties of polar varieties and to [6] for geometric objects similar to the ones we manipulate in a more restrictive context. Our modified

polar varieties are defined incrementally and have a degree which is well controlled (essentially singly exponential in n). Algebraic representations of these modified polar varieties can be computed using many algebraic algorithms for polynomial system solving. Properties of the systems defining these modified polar varieties are exploited by some probabilistic algebraic elimination algorithms (see e.g. the geometric resolution algorithm [31] and references therein) which allows to state our complexity results.

Our implementation is based on Gröbner basis computations which have a good behaviour in practice (see also [29, 77] for preliminary complexity estimates explaining this behaviour). Recall that most of algorithms for computing Gröbner bases are deterministic. This implementation is available at `http://www-polsys.lip6.fr/~greuet/`. We describe it in Section 7; in particular, we show how to check if the generic assumptions required for the correctness are satisfied after performing a linear change of coordinates. We report on experiments showing that its practical performances outperform other implementations of previous algorithms using symbolic computation and can handle non-trivial problems which are difficult from the numerical point of view.

Plan of the paper. We introduce notations and definitions of geometric objects in Section 2. Section 3 describes the algorithm and its subroutines. Section 4 is devoted to the proof of correctness of the algorithm, under some geometric assumptions on some geometric objects depending on the input. Then in Section 5, we prove that these assumptions are true up to a generic change of coordinates on the input. Finally, the complexity is analyzed in Section 6. Some details on the implementation and practical results are presented in Section 7.

2. Notations and Basic Definitions. This section introduces basic geometric objects that our algorithm manipulates. We also make explicit the regularity assumptions that are needed to ensure correctness of the algorithm. It is probabilistic because it requires some generic linear change of variables that are necessary to ensure some properties that are made explicit too.

2.1. Standard notions. We start by defining basic objects we consider in the sequel. Most of the notions presented below are described in detail in [75]. This culminates with the notion of singular and critical points of a polynomial map. In our context, these notions are important since the polynomial map under consideration reaches its extrema at these points.

Algebraic sets. Let $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$. The algebraic variety $V(\mathbf{F})$ is the set $\{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_s(x) = 0\}$. The *Zariski topology* on $\mathbb{C}^n$ is a topology where the closed sets are the algebraic varieties. Given a set $U \subset \mathbb{C}^n$, the Zariski closure of U, denoted by $\overline{U}^{\mathcal{Z}}$, is the closure of U for the Zariski topology. It is the smallest algebraic variety containing U. A Zariski open set is the complement of a Zariski closed set. An algebraic variety V is $\mathbb{Q}$-*reducible* if it can be written as the union of two proper algebraic varieties defined by polynomials with coefficients in $\mathbb{Q}$, *irreducible* else. In this paper, all the algebraic sets we will consider will be defined by polynomials with coefficients in $\mathbb{Q}$; thus the notion of reducibility will refer to $\mathbb{Q}$-reducibility.

For any variety V, there exist irreducible varieties $V_1, \ldots, V_\ell$ such that for $i \neq j$, $V_i \not\subset V_j$ and such that $V = V_1 \cup \cdots \cup V_s$. The algebraic varieties V_i (for $1 \leq i \leq \ell$) are the irreducible components of V. The decomposition of V as the union of its irreducible components is unique. The dimension of $V = V(f_1, \ldots, f_s)$ is the Krull

dimension of its coordinate ring, that is the maximal length of the chains $p_0 \subset p_1 \subset \cdots \subset p_d$ of prime ideals of the quotient ring $\mathbb{C}[\mathbf{X}]/\langle f_1, \ldots, f_s\rangle$ (see [21, Chapter 8]). We write $\dim V = d$. The variety is *equidimensional* of dimension d if and only if its irreducible components have dimension d.

Polynomial mapping and Jacobian matrices. Given $f \in \mathbb{Q}[\mathbf{X}]$, by abuse of notation, we write f for the polynomial mapping $x \mapsto f(x)$. Given $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{Jac}(\mathbf{F})$ is the Jacobian matrix $\left(\frac{\partial f_i}{\partial X_j}\right)_{\substack{1\le i\le s\\ 1\le j\le n}}$. Likewise, $\mathsf{Jac}(\mathbf{F}, k)$ denotes the truncated Jacobian matrix of size $p \times (n-k+1)$ with respect to the variables $X_k, \ldots, X_n$.

Projections. Let $f \in \mathbb{Q}[\mathbf{X}]$ and T be a new indeterminate. For $1 \le i \le n$, $\pi_{\le i}$ is the projection

$$\begin{array}{rcl} V(f-T) \cap (V \times \mathbb{C}) & \longrightarrow & \mathbb{C}^{i+1} \\ (x_1, \ldots, x_n, t) & \longmapsto & (x_1, \ldots, x_i, t). \end{array}$$

For $i = 0$, the projection $\pi_{\le 0}\colon (x_1, \ldots, x_n, t) \longmapsto t$ is denoted by π_T.

Given a set $W \subset \mathbb{C}^n$, the set of non-properness of the restriction of π_T to $(W \times \mathbb{C}) \cap V(f-T)$ is denoted by $\mathsf{NP}(\pi_T, W)$. This is the set of values $t \in \mathbb{C}$ such that for all closed neighbourhoods $\mathcal{O}$ of t (for the euclidean topology), $\pi_T^{-1}(\mathcal{O}) \cap (W \times \mathbb{C}) \cap V(f-T)$ is not closed and bounded.

Change of coordinates. Given $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, $f^{\mathbf{A}}$ (resp. $\mathbf{F}^{\mathbf{A}}$, $V^{\mathbf{A}}$) is the the polynomial $f(\mathbf{AX})$ (resp. the family $\{f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}\}$, the variety $V(\mathbf{F}^{\mathbf{A}})$). We also denote by $f^{\mathbf{A}}$ the polynomial mapping $x \mapsto f^{\mathbf{A}}(x)$. A property on an algebraic set $V(g_1, \ldots, g_p)$ is called generic if there exists a non-empty Zariski open subset of $\mathrm{GL}_n(\mathbb{C})$ such that for all matrices $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$ in this open set, the property holds for $V(g_1^{\mathbf{A}}, \ldots, g_p^{\mathbf{A}})$.

Regular and singular points. The Zariski tangent space to V at $x \in V$ is the vector space T_xV defined by the equations

$$\frac{\partial f}{\partial X_1}(x)v_1 + \cdots + \frac{\partial f}{\partial X_n}(x)v_n = 0,$$

for all polynomials f that vanish on V. If V is equidimensional, the *regular points* on V are the points $x \in V$ where $\dim(T_xV) = \dim(V)$; the *singular points* are all other points. The set of singular points of V is denoted by $\mathsf{Sing}(V)$. If $V = V(\mathbf{F})$ is equidimensional of dimension d then the set of singular points is the set of points in V where the minors of size $n-d$ of $\mathsf{Jac}(\mathbf{F})$ vanish.

Critical points. Assume that $V = V(\mathbf{F})$ is equidimensional of dimension d. A point $x \in V \setminus \mathsf{Sing}(V)$ is a critical point of $f_{|V}$, the restriction of f to V, if it lies in the variety defined by all the minors of size $n-d+1$ of $\mathsf{Jac}([f, \mathbf{F}])$.

We denote by $\mathsf{Crit}(f, V)$ the algebraic variety defined as the vanishing set of

- the polynomials in $\mathbf{F}$,
- and the minors of size $n-d+1$ of $\mathsf{Jac}([f, \mathbf{F}])$.

2.2. Definitions. Our algorithm works under some regularity assumptions that are reasonable from the application viewpoint. These assumptions are based on some rank conditions of the Jacobian matrix of the input constraints $\mathbf{F}$. These rank conditions are sufficient to be able to characterize from $\mathbf{F}$ the critical points of the restriction of the map $x \to f(x)$ to $V(\mathbf{F})$.

We start by defining these regularity assumptions and next, we introduce basic geometric objects (modified polar varieties) that are built upon the notions of singular

and critical points and that we use further to construct objects of dimension at most 1 on which we can "read" the global infimum of a polynomial map.

Assumptions of regularity. Let $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ be a polynomial family such that $\langle \mathbf{F} \rangle$ is radical and $V = V(\mathbf{F})$ is equidimensional of dimension d. In this context, the set of singular points of V is the variety $\mathsf{Sing}(V)$ defined as the vanishing set of

- the polynomials in $\mathbf{F}$,
- and the minors of size $n-d$ of $\mathsf{Jac}(\mathbf{F})$,

The algebraic variety V is *smooth* if $\mathsf{Sing}(V) = \varnothing$.

It is well known that local extrema are critical or singular points. Thus, it is natural to compute them. In order to be able to compute these points, we will assume some properties of regularity on the inputs.

The polynomial family $\mathbf{F}$ satisfies assumptions $\mathbf{R}$ if

- the ideal $\langle \mathbf{F} \rangle$ is radical,
- $V(\mathbf{F})$ is equidimensional of dimension $d > 0$,
- $V(\mathbf{F})$ has finitely many singular points.

Remark that if V satisfies assumptions $\mathbf{R}$ then the variety $\mathsf{Crit}(f, V)$ defined above as the zero-set of minors of the Jacobian matrix of the system is the union of the critical points of $f_{|V}$ and $\mathsf{Sing}(V)$. Hence, it contains all the points at which the local extrema are reached.

In this paper, we consider a polynomial family $\mathbf{F} = \{f_1, \ldots, f_s\}$ that satisfies assumptions $\mathbf{R}$. We denote by V the algebraic variety $V(\mathbf{F})$.

Sample points and modified polar varieties . From a computational point of view, the characterization of critical and singular points as solutions of a polynomial system is not sufficient. When they are in finite number, we will compute parametrizations of these sets.

However, an infimum is not necessarily reached. It can be an asymptotic value, that is the limit of a sequence $f(x_\ell)$, where $(x_\ell)_{\ell \in \mathbb{N}} \subset V \cap \mathbb{R}^n$ tends to infinity.

Our goal is then to construct geometric objects that can be used to compute a parametrization of some critical points and asymptotic values. This is the motivation of the following definition.

DEFINITION 2.1. *For $1 \leq i \leq d-1$, let $\mathscr{C}(f, \mathbf{F}, i)$ be the algebraic variety defined as the vanishing set of*

- *the polynomials in $\mathbf{F}$,*
- *the minors of size $n-d+1$ of $\mathsf{Jac}([f, \mathbf{F}], i+1)$,*
- *and the variables $X_1, \ldots, X_{i-1}$.*

By convention, $\mathscr{C}(f, \mathbf{F}, d) = V \cap V(X_1, \ldots, X_{d-1})$. Let

$$\mathscr{C}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{C}(f, \mathbf{F}, i).$$

For $1 \leq i \leq d-1$, let $\mathscr{P}(f, \mathbf{F}, i) = \overline{\mathscr{C}(f, \mathbf{F}, i) \setminus \mathsf{Crit}(f, V)}^{\mathcal{Z}} \cap \mathsf{Crit}(f, V)$. For $i = d$, let $\mathscr{P}(f, \mathbf{F}, d) = \mathscr{C}(f, \mathbf{F}, d)$. Finally, let

$$\mathscr{P}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{P}(f, \mathbf{F}, i).$$

We will prove that up to a generic linear change of coordinates $\overline{\mathscr{C}(f, \mathbf{F}, i) \setminus \mathsf{Crit}(f, V)}^{\mathcal{Z}}$ (resp. $\mathscr{P}(f, \mathbf{F}, i)$) has dimension at most 1 (resp. 0).

Remark that under assumptions $\mathbf{R}$, $\mathscr{C}(f, \mathbf{F})$ is the union of

- the set of singular points $\mathsf{Sing}(V)$,

- the intersection of $V(X_1, \ldots, X_i)$ and the critical locus of the projection $\pi_{\leq i}$ restricted to $(V \times \mathbb{C}) \cap V(f - T)$, for $1 \leq i \leq d$.

This definition is inspired by the one of the polar varieties (see [4, 5, 7, 68, 69]).

We denote by $\mathscr{S}(\mathbf{F})$ any finite set that contains at least one point in each connected component of $V \cap \mathbb{R}^n$. Such a set can be efficiently computed using e.g. [68].

2.3. Some useful properties. As already mentioned, we will prove that up to a generic change of coordinates, $\mathscr{C}(f, \mathbf{F}) \setminus \mathsf{Crit}(f, V)$ has dimension at most one. From this, we will deduce that the set of asymptotic values of f is the set of non-properness of the restriction to $V(f - T) \cap (\mathscr{C}(f, \mathbf{F}) \times \mathbb{C})$ of the projection π_T. Since $\mathscr{C}(f, \mathbf{F}) \setminus \mathsf{Crit}(f, V)$ has dimension at most one, this set of non-properness is finite and can be computed algorithmically [51, 69].

Moreover, we will prove that up to a generic change of coordinates, $\mathscr{P}(f, \mathbf{F})$ can be used to compute a finite set of points whose image by f contains all the reached local extrema.

In order to identify the global infimum among these values of non-properness and the reached local extrema, some properties are needed. For simplicity, these properties are summarized in the following definition.

DEFINITION 2.2. *Let V be an algebraic set and W be a subset of $\mathbb{R}$, we say that property* $\mathrm{Opt}(W, V)$ *holds if:*

1. *W is finite,*
2. *W contains every local extremum of $f_{|V \cap \mathbb{R}^n}$,*
3. *let $W = \{a_1, \ldots, a_k\}$, $a_0 = -\infty$ and $a_{k+1} = +\infty$. There exists a non-empty Zariski open set $\mathcal{Q} \subset \mathbb{C}$ such that for all $0 \leq i \leq k$ and all couples (t, t') in $]a_i, a_{i+1}[$*

$$f^{-1}(t) \cap V \cap \mathbb{R}^n = \varnothing \iff f^{-1}(t') \cap V \cap \mathbb{R}^n = \varnothing.$$

Now, we define the set $W(f, \mathbf{F})$ (or simply W when there is no ambiguity on $\mathbf{F}$) as the union of $f(\mathscr{S}(\mathbf{F}))$, $f(\mathscr{P}(f, \mathbf{F}))$ and the set of non-properness of the restriction of the projection π_T to $V(f - T) \cap (\mathscr{C}(f, \mathbf{F}) \times \mathbb{C})$. Assuming that $\mathbf{F}$ satisfies $\mathbf{R}$, our goal is to prove that $\mathrm{Opt}(W(f, \mathbf{F}), V)$ is satisfied, up to a generic change of coordinates.

2.4. Genericity properties. In order to do this, we will use some geometric properties that are true up to a generic linear change of coordinates. We define these properties in the next paragraph. Assuming these generic properties, we prove that $\mathrm{Opt}(W(f, \mathbf{F}), V)$ holds in Section 4.

A value $c \in \mathbb{R}$ is isolated in $f(V \cap \mathbb{R}^n)$ if and only if there exists a neighborhood $\mathcal{B}$ of c such that $\mathcal{B} \cap f(V \cap \mathbb{R}^n) = \{c\}$. Given $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$, we consider the following properties.

- $\mathfrak{R}(f, \mathbf{F})$: for all $t \in \mathbb{R} \setminus f(\mathsf{Crit}(f, V) \cup \mathsf{Sing}(V))$, the ideal $\langle \mathbf{F}, f - t \rangle$ is radical, equidimensional and $V(\mathbf{F}, f - t)$ is either smooth of dimension $d - 1$ or is empty.
- $\mathfrak{P}_1(f, \mathbf{F})$: there exists a non-empty Zariski open set $\mathcal{Q} \subset \mathbb{C}$ such that for all $t \in \mathbb{R} \cap \mathcal{Q}$, the restriction of $\pi_{\leq i-1}$ to $V \cap V(f - t) \cap \mathscr{C}(f, \mathbf{F}, i)$ is proper for $1 \leq i \leq d$.
- $\mathfrak{P}_2(f, \mathbf{F})$: for any critical value c of $f_{|V \cap \mathbb{R}^n}$ that is not isolated in $f(V \cap \mathbb{R}^n)$, there exists $x_c \in \mathscr{P}(f, \mathbf{F})$ such that $f(x_c) = c$.

Assume that $\mathbf{F}$ satisfies assumptions $\mathbf{R}$. We will prove that up to a generic change of coordinates, the above properties are satisfied. Properties $\mathfrak{R}(f, \mathbf{F})$ and $\mathfrak{P}_1(f, \mathbf{F})$ will be used to prove that $\mathscr{C}(f, \mathbf{F}) \setminus \mathsf{Crit}(f, V)$ has dimension at most 1 and $\mathscr{P}(f, \mathbf{F})$ is

finite. This implies that the first assertion in Definition 2.2 holds, for the set $W(f, \mathbf{F})$ defined in Section 2.3. They will also be used to prove that the third assertion of Definition 2.2 is satisfied.

Finally, the second assertion of Definition 2.2 will be proved to be satisfied using Properties $\mathfrak{P}_1(f, \mathbf{F})$ and $\mathfrak{P}_2(f, \mathbf{F})$.

Theorem 4.1 establishes that up to generic change of coordinates, properties $\mathfrak{R}(f, \mathbf{F})$, $\mathfrak{P}_1(f, \mathbf{F})$ and $\mathfrak{P}_2(f, \mathbf{F})$ hold.

3. Algorithm. This section is structured as follows. After an outline of the algorithm, we explain its specification. Next, we describe the subroutines it uses and this section ends with a formal description of the algorithm.

3.1. Outline. There are basically two main steps in our algorithm. After a generic change of coordinates, the first one is the computation of finite sets from which a set containing all the local extrema of $f_{|V \cap \mathbb{R}^n}$ can be recovered by deciding the emptiness of real algebraic sets. Reusing the notations in the previous section, these sets are the following:

- a set $\mathscr{S}(\mathbf{F})$ of sample points of $V(\mathbf{F}) \cap \mathbb{R}^n$,
- the set $\mathscr{P}(f, \mathbf{F}) \cap \mathbb{R}^n$,
- and the set of non-properness of the restriction to $V(f - T) \cap (\mathscr{C}(f, \mathbf{F}) \times \mathbb{C})$ of the projection π_T.

Let $W = W(f, \mathbf{F})$ be defined as the union of the above set of non-properness, $f(\mathscr{S}(\mathbf{F}))$ and $f(\mathscr{P}(f, \mathbf{F}) \cap \mathbb{R}^n)$. We prove in Section 4 that Property $\mathrm{Opt}(W, V)$ holds. In particular, this means that W contains all the local extrema of $f_{|V \cap \mathbb{R}^n}$ and is finite.

The second main step of the algorithm is then to detect the global infimum among the values in W. By definition, $f^\star$ is the smallest value c in $V \cap \mathbb{R}^n$ such that

1. if $t < c$ then $t \notin f(V \cap \mathbb{R}^n)$ and
2. for all $t \geq c$, $[c, t]$ meets $f(V \cap \mathbb{R}^n)$.

Let $a_1 < \cdots < a_k$ be the values in W, let $a_0 = -\infty$ and $a_{k+1} = +\infty$.

If $f^\star = -\infty$, then for any value $t \in]-\infty, a_1[$, $f^{-1}(t) \cap V \cap \mathbb{R}^n$ is not empty. This can be decided using any algorithm for deciding the emptiness of real algebraic sets.

Now, let $0 \leq i \leq k+1$ and assume that the infimum $f^\star$ is not $a_0, \ldots, a_{i-1}$. Since W contains all the local extrema, $f^\star \geq a_i$. If a_i lies in $f(\mathscr{S}(\mathbf{F}))$ or in $f(\mathscr{P}(f, \mathbf{F}) \cap \mathbb{R}^n)$ then this is a value attained by f. In this case, $f^\star$ is necessarily a_i.

Else, if a_i is an asymptotic value then there are values attained by f in every neighborhood of a_i. Since $f^\star \geq a_i$, the third assertion of Property $\mathrm{Opt}(W, V)$ implies that for almost all $t \in]a_i, a_{i+1}[$, t is a value attained by f. In particular, if a_i is an asymptotic value then for a random number $t \in]a_i, a_{i+1}[$, the variety $V(f - t) \cap V(\mathbf{F}) \cap \mathbb{R}^n$ is non-empty. Thus, if $V(f - t) \cap V(\mathbf{F}) \cap \mathbb{R}^n$ is not empty for a random value t in $]a_i, a_{i+1}[$ then a_i is an asymptotic value, that is necessarily $f^\star$. Else, a_i is not relevant for the optimization problem under consideration and we have $f^\star \geq a_{i+1}$.

3.2. Specifications. In the descriptions of the algorithms, algebraic sets are represented with polynomial families that define them and ideals are represented by a finite list of generators (e.g. a Gröbner basis).

Let $Z \subset \mathbb{R}^n$ be a finite real algebraic set defined by polynomials in $\mathbb{Q}[\mathbf{X}]$. It can be represented by a rational parametrization, that is a sequence of polynomials $q, q_0, q_1, \ldots, q_n \in \mathbb{Q}[U]$ such that for all $x = (x_1, \ldots, x_n) \in Z$, there exists $u \in \mathbb{R}$ such

that

$$\left\{\begin{array}{rcl} q(u) & = & 0 \\ x_1 & = & q_1(u)/q_0(u) \\ & \vdots & \\ x_n & = & q_n(u)/q_0(u) \end{array}\right.$$

with the convention that $q = 1$ when $Z = \varnothing$. Moreover, a single point in Z can be represented using isolating intervals. Note that such a representation can be computed from a Gröbner basis [27, 28, 26, 63] and algorithms computing such a representation are implemented in computer algebra systems.

Also, a real algebraic number α is represented by a univariate polynomial P and an isolating interval I.

3.3. Subroutines. In this paragraph we describe the main subroutines SetContainingLocalExtrema and FindInfimum that will are used in the main algorithm. They correspond to the two main steps sketched in Section 3.1.

We start with some standard subroutines on which these both subroutines are based. Given a univariate polynomial P, we denote by $\mathrm{Roots}_{\mathbb{R}}(P)$ the set of its real roots.

RealSamplePoints. Given $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, RealSamplePoints returns a list of equations ListSamplePoints $\subset \mathbb{Q}[\mathbf{X}]$ such that $V(\mathsf{ListSamplePoints})$ contains at least one point in each connected component of $V(\mathbf{F}) \cap \mathbb{R}^n$. We refer to [68] and references therein for an efficient algorithm performing this task.

SetOfNonProperness. The routine SetOfNonProperness takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{G} \subset \mathbb{Q}[\mathbf{X}]$ such that $\dim V(\mathbf{G}) \leq 1$. It returns a univariate polynomial in T whose set of roots contains the set of non-properness of the restriction of π_T to $V(f - T) \cap (V(\mathbf{G}) \times \mathbb{C})$. Such an algorithm is given in [51, 69].

RealRootIsolation. Given $P \in \mathbb{Q}[T]$ whose set of real roots is $a_1 < \cdots < a_k$, this routine returns a sorted list of k pairwise disjoint intervals with rational endpoints $[q_i, q_{i+1}]$ such that $a_i \in [q_i, q_{i+1}]$ (since the intervals are disjoint, the list is sorted for the natural order : $[a, b] < [c, d]$ if and only if $b < c$). We refer to [9, 65] for an algorithm with this specification.

IsEmpty. Given $\mathbf{G} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, this routine returns either true if $V(\mathbf{G}) \cap \mathbb{R}^n$ is empty of false if it is nonempty. This is a weakened variant of RealSamplePoints.

SetContainingLocalExtrema. It takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, $\mathfrak{P}_1(f, \mathbf{F})$, $\mathfrak{P}_2(f, \mathbf{F})$ and $\mathfrak{R}(f, \mathbf{F})$. We denote by V the algebraic set defined by $\mathbf{F}$.

It returns a list ListSamplePoints $\subset \mathbb{Q}[\mathbf{X}]$, a list ListCriticalPoints $\subset \mathbb{Q}[\mathbf{X}]$ and a polynomial $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ such that the property

$$\mathrm{Opt}\left(f\left(V\left(\mathsf{ListSamplePoints}\right)\right) \cup f\left(V\left(\mathsf{ListCriticalPoints}\right)\right) \cup \mathrm{Roots}_{\mathbb{R}}\left(P_{\mathsf{NP}}\right), V\right)$$

holds. The list of polynomials ListSamplePoints and ListCriticalPoints represent respectively at least one point in each connected component of $V \cap \mathbb{R}^n$ and the set of critical points of the restriction of the map $x \to f(x)$ to V and some fibers.

SetContainingLocalExtrema$(f, \mathbf{F})$

- $\mathsf{ListSamplePoints} \leftarrow \mathsf{RealSamplePoints}(\mathbf{F})$;
- $P_{\mathsf{NP}} \leftarrow 1$;
- for $1 \leq i \leq d$ do
  - $\mathsf{L_{sat}}[i] \leftarrow$ a list of equations defining $\overline{\mathscr{C}(f, \mathbf{F}, i) \setminus \mathsf{Crit}(f, V(\mathbf{F}))}^{\mathcal{Z}}$;
  - $P_{\mathsf{NP}} \leftarrow$ the univariate polynomial $P_{\mathsf{NP}} \times \mathsf{SetOfNonProperness}(f, \mathsf{L_{sat}}[i])$;
  - $\mathsf{ListCriticalPoints}[i] \leftarrow$ a list of equations defining $\mathscr{P}(f, \mathbf{F}, i)$.
- return $(\mathsf{ListSamplePoints}, \mathsf{ListCriticalPoints}, P_{\mathsf{NP}})$;

Its correctness is stated in Proposition 4.2. Its proof relies on intermediate results given in Section 4.1.

FindInfimum. The routine FindInfimum takes as input:

- $f \in \mathbb{Q}[\mathbf{X}]$,
- $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$ and $\mathfrak{R}(f, \mathbf{F})$; we let $V \subset \mathbb{C}^n$ be the algebraic set it defines,
- $\mathsf{ListSamplePoints} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{ListCriticalPoints} \subset \mathbb{Q}[\mathbf{X}]$ and $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ such that $\mathrm{Opt}(f(V(\mathsf{ListSamplePoints})) \cup f(V(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}}), V)$ holds.

It returns

- $+\infty$ if $V(\mathbf{F}) \cap \mathbb{R}^n$ is empty;
- $-\infty$ if f is not bounded below on $V(\mathbf{F}) \cap \mathbb{R}^n$;
- if $f^\star$ is finite and not reached: $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ and an interval I isolating $f^\star$;
- if $f^\star$ is reached, a rational parametrization encoding $x^\star$ and $f^\star = f(x^\star)$.

$\mathsf{FindInfimum}(f, \mathbf{F}, \mathsf{ListSamplePoints}, \mathsf{ListCriticalPoints}, P_{\mathsf{NP}})$

- $a_1 < \cdots < a_k \leftarrow f(V(\mathsf{ListSamplePoints})) \cup f(V(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}})$;
- $a_{k+1} = +\infty$;
- $q_0 \leftarrow$ a random rational $< a_1$;
- if $\mathsf{IsEmpty}(\{f - q_0, \mathbf{F}\})$=false then
  - return $-\infty$;
- $i \leftarrow 1$;
- while $i \leq k$ do
  - if $a_i \in f(V(\mathsf{ListSamplePoints})) \cup f(V(\mathsf{ListCriticalPoints}))$ then
    - RP $\leftarrow$ a rational parametrization encoding a minimizer $x^\star$ and $f(x^\star) = a_i$;
    - return RP

    else
    - $q_i \leftarrow$ a random rational in $]a_i, a_{i+1}[$;
    - if $\mathsf{IsEmpty}(\{f - q_i, \mathbf{F}\})$=false then
      - return $(P_{\mathsf{NP}},]q_{i-1}, q_i[)$

      else
      - $i \leftarrow i + 1$
- return a_{k+1}

Its correctness is stated by Proposition 4.6 whose proof is in Section 4.6.

By assumption on the inputs, $V(\mathsf{ListSamplePoints}) \cup V(\mathsf{ListCriticalPoints})$ is finite. As explained in Section 3.2, a single point x that lies in this variety can be represented by a rational parametrization $q, q_0, q_1, \ldots, q_n$ and an interval isolating the corresponding root of q. From this parametrization and the isolating interval, an interval isolating $f(x)$ can be computed. Likewise, the roots of P_{NP} are represented by

isolating intervals. These intervals can be computed such that they do not intersect. Hence, they can be sorted so that the i-th interval corresponds to a_i.

Then, testing whether $a_i \in f\left(V\left(\mathsf{ListSamplePoints}\right)\right) \cup f\left(V\left(\mathsf{ListCriticalPoints}\right)\right)$ is done by testing whether the interval corresponding with a_i comes from the parametrization of $V\left(\mathsf{ListSamplePoints}\right) \cup V\left(\mathsf{ListCriticalPoints}\right)$. If so, the parametrization and the isolating interval of q corresponding with a_i are an encoding for a_i and a point x_{a_i} such that $f\left(x_{a_i}\right) = a_i$.

3.4. Main Algorithm. The main routine Optimize takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$. It returns

- $+\infty$ if $V\left(\mathbf{F}\right) \cap \mathbb{R}^n$ is empty;
- $-\infty$ if f is not bounded below on $V\left(\mathbf{F}\right) \cap \mathbb{R}^n$;
- if $f^\star$ is finite and not reached: $P_{\mathsf{NP}} \in \mathbb{Q}\left[T\right]$ and an interval I isolating $f^\star$;
- if $f^\star$ is reached, a rational parametrization encoding $x^\star$ and $f^\star = f\left(x^\star\right)$.

$\mathsf{Optimize}(f, \mathbf{F})$.

- $\mathbf{A} \leftarrow$ a random matrix in $\mathrm{GL}_n(\mathbb{Q})$;
- $(\mathsf{ListSamplePoints}, \mathsf{ListCriticalPoints}, P_{\mathsf{NP}}) \leftarrow \mathsf{SetContainingLocalExtrema}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$;
- $\mathsf{Infimum} \leftarrow \mathsf{FindInfimum}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, \mathsf{ListSamplePoints}, \mathsf{ListCriticalPoints}, P_{\mathsf{NP}}\right)$;
- return Infimum.

---

4. Proof of correctness. We first assume the following theorem, it is proved in Section 5. It states that the properties $\mathfrak{R}\left(f, \mathbf{F}\right)$, $\mathfrak{P}_1\left(f, \mathbf{F}\right)$ and $\mathfrak{P}_2\left(f, \mathbf{F}\right)$ defined in Section 2.4 are satisfied up to a generic change of coordinates.

THEOREM 4.1. *Let $f \in \mathbb{Q}\left[\mathbf{X}\right]$ and $\mathbf{F} \subset \mathbb{Q}\left[\mathbf{X}\right]$ satisfying assumptions $\mathbf{R}$. There exists a non-empty Zariski open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, the properties $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold.*

Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski open set given in Theorem 4.1. We prove in the sequel that if the random matrix chosen in Optimize lies in $\mathscr{O}$ then Optimize is correct.

The correctness of Optimize is a consequence of the correctness of the subroutines SetContainingLocalExtrema and FindInfimum. The correctness of SetContainingLocalExtrema is given in Section 4.1 below. The proof of correctness of FindInfimum is given in Section 4.2 page 15.

4.1. Correctness of SetContainingLocalExtrema. We first state the correctness of $\mathsf{SetContainingLocalExtrema}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$.

PROPOSITION 4.2. *Let $f \in \mathbb{Q}\left[\mathbf{X}\right]$ and $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}\left[\mathbf{X}\right]$ satisfying assumptions $\mathbf{R}$. Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski open set defined in Theorem 4.1. Then for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, $\mathsf{SetContainingLocalExtrema}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ returns a list $\mathsf{ListSamplePoints} \subset \mathbb{Q}\left[\mathbf{X}\right]$, a list $\mathsf{ListCriticalPoints} \subset \mathbb{Q}\left[\mathbf{X}\right]$ and a polynomial $P_{\mathsf{NP}} \in \mathbb{Q}\left[T\right]$ such that the property*

$$\mathrm{Opt}\left(f^{\mathbf{A}}\left(V\left(\mathsf{ListSamplePoints}\right)\right) \cup f^{\mathbf{A}}\left(V\left(\mathsf{ListCriticalPoints}\right)\right) \cup \mathrm{Roots}_{\mathbb{R}}\left(P_{\mathsf{NP}}\right), V^{\mathbf{A}}\right)$$

holds.

Given $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, let $W^{\mathbf{A}}$ be the set of values

$$W^{\mathbf{A}} = f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right) \cup f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right) \cup \mathsf{NP}\left(\pi_T, \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}\right) \subset \mathbb{C}$$

with $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right) = V\left(\mathsf{ListSamplePoints}\right)$ and $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) = V\left(\mathsf{ListCriticalPoints}\right)$ and $\mathrm{Roots}_{\mathbb{R}}\left(P_{\mathsf{NP}}\right) = \mathsf{NP}\left(\pi_T, \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$.

We start by establishing that $\mathrm{Opt}\left(W^{\mathbf{A}}, V^{\mathbf{A}}\right)$ holds: we prove below that $W^{\mathbf{A}}$ contains all the local extrema (Proposition 4.3), that it is finite (Proposition 4.4) and the last assertion in Definition 2.2 (Proposition 4.5). Finally, we conclude with the proof of Proposition 4.2 page 15.

Since $V^{\mathbf{A}}$ is an algebraic variety, the image $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ is a semi-algebraic subset of $\mathbb{R}$. Hence, it is a finite union of real disjoint intervals. They are either of the form $[b_i, b_{i+1}]$, $[b_i, b_{i+1}[$, $]b_i, b_{i+1}]$ or $\{b_i\}$, for some $b_0 \in \mathbb{R} \cup \{-\infty\}$, $b_1, \ldots, b_r \in \mathbb{R}$ and $b_{r+1} \in \mathbb{R} \cup \{+\infty\}$. Then the local extrema of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ are the b_i's. If b_i is an endpoint included in the interval, then it is reached, meaning that it is either a minimum or a maximum. If the interval is a single point then b_i is isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$. Else, it is not isolated. If b_i is an endpoint that is not included in the interval, then $b_i \notin f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ is an extremum that is not reached. Remark that our goal is to find b_0, that is equal to $f^\star$.

PROPOSITION 4.3. *Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski open set defined in Theorem 4.1. For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, and any local extremum $\ell \in \mathbb{R}$ of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$, the following holds.*

1. *If ℓ is a value that is isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ then $\ell \in f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right)$;*
2. *if ℓ is a value that is not isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ such that there exists $x_\ell \in V^{\mathbf{A}} \cap \mathbb{R}^n$ with $f^{\mathbf{A}}(x_\ell) = \ell$ then $\ell \in f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$;*
3. *if $\ell \notin f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ then $\ell \in \mathsf{NP}\left(\pi_T, \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$.*

As a consequence, every local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ is contained in $W^{\mathbf{A}}$.

Proof. Let $\ell \in \mathbb{R}$ be a local extremum.

Case 1. Since ℓ is isolated, there exists $x_\ell \in V^{\mathbf{A}} \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}(x_\ell) = \ell$. Let $C^{\mathbf{A}}$ be the connected component of $V^{\mathbf{A}} \cap \mathbb{R}^n$ containing x_ℓ. We prove that $f^{\mathbf{A}}$ is constant on $C^{\mathbf{A}}$. Let $x' \in C^{\mathbf{A}}$ and assume that $f^{\mathbf{A}}(x') \neq \ell$. Since ℓ is isolated, there exists a neighborhood $\mathcal{B}$ of ℓ such that $f^{\mathbf{A}}\left(C^{\mathbf{A}}\right)$ is the union of $\{\ell\}$ and some set S that contains $f^{\mathbf{A}}(x')$ but does not meet $\mathcal{B}$. In particular, $f^{\mathbf{A}}\left(C^{\mathbf{A}}\right)$ is not connected. This is a contradiction since $f^{\mathbf{A}}$ is continuous and $C^{\mathbf{A}}$ connected.

The set $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)$ is a set containing at least one point in each connected component of $V^{\mathbf{A}} \cap \mathbb{R}^n$. In particular it contains a point y in the connected component $C^{\mathbf{A}}$ of x_ℓ. Since the restriction of $f^{\mathbf{A}}$ to $C^{\mathbf{A}}$ is constant, $f^{\mathbf{A}}(y) = \ell$, so that $\ell \in f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right)$.

Case 2. Since $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, property $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds (Theorem 4.1). This means that there exists $x_\ell \in \mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ such that $f^{\mathbf{A}}(x_\ell) = \ell$, that is $\ell \in f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$.

Case 3. If $\ell \notin f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, by definition, as a local extremum, there exists a closed neighborhood $\mathcal{U}$ of ℓ such that we can construct a sequence $(x^{(k)})_{k \in \mathbb{N}} \subset \left(f^{\mathbf{A}}\right)^{-1}(\mathcal{U}) \cap V^{\mathbf{A}} \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}\left(x^{(k)}\right) \to \ell$. We first prove that we can not extract a converging subsequence from $(x^{(k)})$. Indeed, assume that there exists a converging subsequence $(x'^{(k)})$ and denote by x its limit. Since $V^{\mathbf{A}} \cap \mathbb{R}^n$ and $\left(f^{\mathbf{A}}\right)^{-1}(\mathcal{U}) \cap \mathbb{R}^n$ are closed sets for the euclidean topology, x lies in $\left(f^{\mathbf{A}}\right)^{-1}(\mathcal{U}) \cap V^{\mathbf{A}} \cap \mathbb{R}^n$.

As a subsequence of $f^{\mathbf{A}}\left(x^{(k)}\right)$, the sequence $f^{\mathbf{A}}\left(x'^{(k)}\right)$ tends to ℓ. Moreover, by continuity of $f^{\mathbf{A}}$, $f^{\mathbf{A}}\left(x'^{(k)}\right)$ tends to $f^{\mathbf{A}}(x)$. This implies that $f^{\mathbf{A}}(x) = \ell$, that is ℓ is attained, which is a contradiction. Since this is true for any converging subsequence $(x'^{(k)})$ of $(x^{(k)})$, this implies that $(x^{(k)})$ can not be bounded. Finally, this proves that $\|(x^{(k)})\|$ tends to ∞.

Let $\varepsilon > 0$. There exists $k_0 \in \mathbb{N}$ such that for all $k \geq k_0$, $f^{\mathbf{A}}\left(x^{(k)}\right) \in [\ell - \varepsilon, \ell + \varepsilon]$.

By construction of $x^{(k)}$, $\left(f^{\mathbf{A}}\right)^{-1}\left(f^{\mathbf{A}}\left(x^{(k)}\right)\right) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing$.

By assumption, we have $\mathbf{A} \in \mathscr{O}$; then Theorem 4.1 implies that $\mathfrak{R}\left(\mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold. Thus [33, Proposition 1.3] ensures that for all $t \in \mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$, $V^{\mathbf{A}} \cap V\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is empty if and only if $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap V\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is empty. Since $\mathbb{R} \setminus \mathcal{Q}^{\mathbf{A}}$ is finite, one can assume without loss of generality that for all k, $f^{\mathbf{A}}\left(x^{(k)}\right) \in \mathcal{Q}^{\mathbf{A}}$.

Then $\left(f^{\mathbf{A}}\right)^{-1}\left(f^{\mathbf{A}}\left(x^{(k)}\right)\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n \neq \varnothing$. Picking up a point $\widetilde{x}^{(k)}$ in this last set, for each $k \geq k_0$, leads to the construction of a sequence of points $\left(\widetilde{x}^{(k)}\right)$ in $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ such that $f\left(\widetilde{x}^{(k)}\right)$ tends to ℓ. Since $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \subset V^{\mathbf{A}}$ and ℓ is not reached, this sequence is unbounded. Since $f^{\mathbf{A}}\left(\mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)\right)$ is finite by Sard's theorem, one can assume without loss of generality that for all k, $\widetilde{x}^{(k)} \notin \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$.

Then considering the sequence $\left(\widetilde{x}^{(k)}, t = f^{\mathbf{A}}\left(\widetilde{x}^{(k)}\right)\right)$ proves that π_T restricted to $V\left(f^{\mathbf{A}} - T\right) \cap \left(\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}} \times \mathbb{C}\right)$ is not proper at ℓ; in other words $\ell \in \mathsf{NP}\left(\pi_T, \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$. □

Proposition 4.4. *For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, the set $W^{\mathbf{A}}$ is finite.*

Proof. Recall that, by definition, $W^{\mathbf{A}} = f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right) \cup f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right) \cup \mathsf{NP}\left(\pi_T, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$. We prove below the following assertions.

1. $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)$ is finite,
2. For $1 \leq i \leq d$, $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is finite and
3. $\mathsf{NP}\left(\pi_T, \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$ is finite.

Assertion 1. The first assertion is true for all $\mathbf{A}$, since by assumption, $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)$ is a finite set.

Assertion 2. Let $1 \leq i \leq d$. Recall that

$$\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) = \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}} \cap \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right).$$

We first prove that $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension 1. Next, it will be easy to deduce that its intersection with $\mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$ has dimension at most 0.

By assumption, we have $\mathbf{A} \in \mathscr{O}$. Thus, Theorem 4.1 implies that $\mathfrak{R}\left(\mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold. Thus [33, Proposition 1.3] ensures that for all $t \in \mathcal{Q}^{\mathbf{A}}$, the algebraic set $V\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ has dimension at most zero.

Now, let $Z^{\mathbf{A}}$ be an irreducible component of $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. In particular, $Z^{\mathbf{A}}$ is an irreducible component of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ that is not contained in $\mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$. Consider the restriction $f^{\mathbf{A}}_{|Z^{\mathbf{A}}} \colon Z^{\mathbf{A}} \longrightarrow \mathbb{C}$. Its image has a Zariski closure of dimension 0 or 1.

Assume first that $f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ is 0-dimensional. Then as a continuous function, $f^{\mathbf{A}}_{|Z^{\mathbf{A}}}$ is locally constant. This implies that $Z^{\mathbf{A}}$ is contained in the critical locus of $f^{\mathbf{A}}_{|V^{\mathbf{A}}}$. In particular, this means that $Z^{\mathbf{A}} \subset \mathsf{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$, which is a contradiction.

Then all irreducible components $Z^{\mathbf{A}}$ are such that $\overline{f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension 1. From the Theorem on the dimension of fibers ([75, Theorem 7, Chapter 1, pp. 76]), there exists a Zariski open set $U \subset \mathbb{C}$ such that for all $y \in U$, $\dim\left(f^{\mathbf{A}}\right)^{-1} = \dim Z^{\mathbf{A}} - 1$. In particular if t lies in the non-empty Zariski open set $U \cap \mathcal{Q}^{\mathbf{A}}$, the following holds

$$0 \geq \dim\left(f^{\mathbf{A}}\right)^{-1} = \dim Z^{\mathbf{A}} - 1.$$

Then every irreducible component $Z^{\mathbf{A}}$ of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension ≤ 1, so that $\dim \overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\leq 1$.

Now, let $Z_1^{\mathbf{A}}\cup\cdots\cup Z_\alpha^{\mathbf{A}}\cup\cdots\cup Z_\beta^{\mathbf{A}}$ be the decomposition of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ as a union of irreducible components. Up to reordering, assume that

- for $1\leq i\leq \alpha$, $Z_i^{\mathbf{A}}\not\subset \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$,
- for $\alpha+1\leq j\leq \beta$, $Z_i^{\mathbf{A}}\subset \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$.

Then the decomposition of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ as a union of irreducible components is $Z_1^{\mathbf{A}}\cup\cdots\cup Z_\alpha^{\mathbf{A}}$.

Let $1\leq i\leq \alpha$ and consider $Z_i^{\mathbf{A}}\cap \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. If it is non-empty, since $Z_i^{\mathbf{A}}\not\subset \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$, [48, Corollary 3.2 p. 131] implies that $Z_i^{\mathbf{A}}\cap \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$ has dimension less than or equal to $\dim Z_i^{\mathbf{A}}-1\leq 1-1=0$. Finally, this proves that $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\cap \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$ has dimension ≤ 0.

Assertion 3. Since $\mathbf{A}\in\mathscr{O}$, Theorem 4.1 implies that $\mathfrak{R}\left(\mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_1\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)$ hold. We have proved above, that for $1\leq i\leq d$, $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension at most 1.

Then by [44, Theorem 3.8], each set $\mathsf{NP}\left(\pi_T,\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$ has dimension at most 0, thus $\mathsf{NP}\left(\pi_T,\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$ is finite.

To conclude, we prove that the set of values $t\in\mathbb{C}$ such that there exists a sequence $(x^{(k)})_{k\in\mathbb{N}}\subset \overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}$ satisfying $\lim\limits_{k\to+\infty}||x^{(k)}||=+\infty$ and $\lim\limits_{k\to+\infty}f^{\mathbf{A}}(x^{(k)})=t$ is exactly the set $\mathsf{NP}\left(\pi_T,\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$.

Let $t_0\in\mathbb{C}$ and $\left(x^{(k)}\right)=\left(x_1^{(k)},\ldots,x_n^{(k)}\right)$ be a sequence of points in the set $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}$ such that $\lim\limits_{k\to+\infty}\left\|x^{(k)}\right\|=+\infty$ and $\lim\limits_{k\to+\infty}f^{\mathbf{A}}\left(x^{(k)}\right)=t_0$.

Let $\varepsilon>0$. There exists $N\in\mathbb{N}$ such that for all $k\geq N$, $\left|f^{\mathbf{A}}\left(x^{(k)}\right)-t_0\right|\leq\varepsilon$. In particular, for all $k\geq N$, $\left(f^{\mathbf{A}}\right)\left(x^{(k)}\right)$ lies in the closed ball $\overline{B}\left(t_0,\varepsilon\right)$. This means that $\pi_T^{-1}\left(\overline{B}\left(t_0,\varepsilon\right)\right)\cap V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\times\mathbb{C}\right)$ contains all the points

$$\left(x_1^{(k)},\ldots,x_n^{(k)},t=f^{\mathbf{A}}\left(x^{(k)}\right)\right)$$

for $k\geq N$. Since $\left(x^{(k)}\right)$ is not bounded, we deduce that

$$\pi_T^{-1}\left(\overline{B}\left(t_0,\varepsilon\right)\cap V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)\times\mathbb{C}\right)$$

is not bounded. This means that t_0 is a point where the projection π_T restricted to $V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\times\mathbb{C}\right)$ is not proper.

Conversely, if $t_0\in\mathbb{C}$ is such that for all $\varepsilon>0$,

$$\pi_T^{-1}\left(\overline{B}\left(t_0,\varepsilon\right)\cap V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)\times\mathbb{C}\right)$$

is not bounded, we can construct by induction a sequence $\left(\left(x^{(k)},f^{\mathbf{A}}\left(x^{(k)}\right)\right)\right)_{k\in\mathbb{N}}$ such that:

- for all $k \in \mathbb{N}$, the point $\left(x^{(k)}, f^{\mathbf{A}}\left(x^{(k)}\right)\right)$ lies in

$$\pi_T^{-1}\left(\overline{B}\left(t_0, \frac{1}{k}\right) \cap V\left(f^{\mathbf{A}} - T\right) \cap \left(\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}\right) \times \mathbb{C}\right);$$

- for all $k \in \mathbb{N}$, $\|x_{k+1}\| > 2\left\|x^{(k)}\right\|$.

In particular, $\left(x^{(k)}\right)_{k\in\mathbb{N}} \subset \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathsf{Crit}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)}^{\mathcal{Z}}$, $\lim_{k\to+\infty} \left\|x^{(k)}\right\| = +\infty$ and $\lim_{k\to+\infty} f^{\mathbf{A}}(x^{(k)}) = t_0$. □

PROPOSITION 4.5. *For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, let $W^{\mathbf{A}} = \{a_1, \ldots, a_k\}$, $a_0 = -\infty$ and $a_{k+1} = +\infty$ with $a_i < a_{i+1}$ for $0 \leq i \leq k$. There exists a non-empty Zariski open set $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ such that for all $0 \leq i \leq k$ and all couples (t, t') in $]a_i, a_{i+1}[$*

$$f^{-1}(t) \cap V \cap \mathbb{R}^n = \varnothing \Longleftrightarrow f^{-1}(t') \cap V \cap \mathbb{R}^n = \varnothing.$$

Proof. Our proof is by contradiction. Assume that there exists i such that there exists $a \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$ such that $f^{\mathbf{A}^{-1}}(a) \cap V^{\mathbf{A}} \cap \mathbb{R}^n = \varnothing$ and $b \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$ such that $f^{\mathbf{A}^{-1}}(b) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing$. Without loss of generality, we can assume that $a < b$ and

$$b = \inf\left\{t \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}} \text{ s.t.} f^{\mathbf{A}^{-1}}(t) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing\right\}.$$

Then b is a local infimum of $f^{\mathbf{A}}_{|V^{\mathbf{A}}\cap\mathbb{R}^n}$ that is neither a_i nor a_{i+1}. However, according to Proposition 4.3, b lies in $W^{\mathbf{A}}$. Hence there exists i such that $b = a_i$, which is a contradiction. □

We can now give the proof of Proposition 4.2 using the above propositions.

Proof. Let $\mathsf{ListSamplePoints} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{ListCriticalPoints} \subset \mathbb{Q}[\mathbf{X}]$ and $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ be the output of $\mathsf{SetContainingLocalExtrema}(f, \mathbf{F})$. Denote by W the set

$$f(V(\mathsf{ListSamplePoints})) \cup f(V(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}}).$$

The routine $\mathsf{SetContainingLocalExtrema}$ is correct if property $\mathrm{Opt}(W, V)$ holds (see Definition 2.2). Then we check that

1. every local extremum of $f_{|V\cap\mathbb{R}^n}$ is contained in W,
2. W is finite,
3. let $W = \{a_1, \ldots, a_k\}$, $a_0 = -\infty$ and $a_{k+1} = +\infty$ with $a_i < a_{i+1}$ for $0 \leq i \leq k$. There exists a non-empty Zariski open set $\mathcal{Q} \subset \mathbb{C}$ such that for all $0 \leq i \leq k$ and all couples (t, t') in $]a_i, a_{i+1}[$

$$f^{-1}(t) \cap V \cap \mathbb{R}^n = \varnothing \Longleftrightarrow f^{-1}(t') \cap V \cap \mathbb{R}^n = \varnothing.$$

Proposition 4.3 establishes the assertion 1. Assertion 2 is a restatement of Proposition 4.4. Assertion 3 is established by Proposition 4.5. □

4.2. Correctness of $\mathsf{FindInfimum}$**.** Finally, we prove the correctness of the routine $\mathsf{FindInfimum}$.

PROPOSITION 4.6. *Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, $f \in \mathbb{Q}[\mathbf{X}]$, $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, $\mathsf{ListSamplePoints}^{\mathbf{A}} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{ListCriticalPoints}^{\mathbf{A}} \subset \mathbb{Q}[\mathbf{X}]$ and $P^{\mathbf{A}}_{\mathsf{NP}} \in \mathbb{Q}[T]$. Let $W^{\mathbf{A}} = \{a_1, \ldots, a_k\}$, be the finite algebraic set*

$$f^{\mathbf{A}}\left(V\left(\mathsf{ListSamplePoints}^{\mathbf{A}}\right)\right) \cup f\left(V\left(\mathsf{ListCriticalPoints}^{\mathbf{A}}\right)\right) \cup \mathrm{Roots}_{\mathbb{R}}\left(P^{\mathbf{A}}_{\mathsf{NP}}\right),$$

and assume that $\mathrm{Opt}\left(W^{\mathbf{A}}, V^{\mathbf{A}}\right)$ *is satisfied. Then let* $a_0 = -\infty$, $a_{k+1} = +\infty$ *and let* $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ *be the Zariski open set such that, for all* $0 \leq i \leq k$ *all couples* (t, t') *in* $]a_i, a_{i+1}[$

$$f^{-1}(t) \cap V \cap \mathbb{R}^n = \varnothing \iff f^{-1}(t') \cap V \cap \mathbb{R}^n = \varnothing.$$

If the random rational numbers computed in FindInfimum *lie in* $\mathcal{Q}^{\mathbf{A}}$ *then* FindInfimum *is correct.*

Proof. Since $\mathbf{A} \in \mathscr{O}$, Theorem 4.1 implies that property $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ is satisfied. Hence IsEmpty is always called with a correct input.

Assume first that $f^\star = -\infty$. By assertion 3 of $\mathrm{Opt}\left(W^{\mathbf{A}}, V^{\mathbf{A}}\right)$ (see Definition 2.2), the fiber of $f^{\mathbf{A}}$ at a rational $q_0 \in \mathcal{Q}^{\mathbf{A}} \cap \mathbb{Q}$ such that $q_0 < a_1$ is not empty. Hence the first call to IsEmpty returns false so that FindInfimum returns $-\infty$. Now, remark that if FindInfimum returns $-\infty$, then assertion 3 of $\mathrm{Opt}\left(W^{\mathbf{A}}, V^{\mathbf{A}}\right)$ implies that $f^\star = -\infty$.

If $f^\star$ is finite, because the second assertion of $\mathrm{Opt}\left(W^{\mathbf{A}}, V^{\mathbf{A}}\right)$ holds, it is sufficient to identify the smallest local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ in $W^{\mathbf{A}}$. To this end, we want to detect an eventual redundant value in $W^{\mathbf{A}}$. Such a redundant value, say a_i, is such that the interval $[a_i, a_{i+1}[$ does not contain any value reached by $f^{\mathbf{A}}$. In particular, it is a value that is not in $f^{\mathbf{A}}\left(V\left(\mathsf{ListSamplePoints}^{\mathbf{A}}\right)\right) \cup f\left(V\left(\mathsf{ListCriticalPoints}^{\mathbf{A}}\right)\right)$ and such that $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ does not reach any value in the interval $]a_i, a_{i+1}[$. Because of assertion 3 of $\mathrm{Opt}\left(W^{\mathbf{A}}, V^{\mathbf{A}}\right)$, testing this last point is equivalent to test the emptiness of the real fiber of $f^{\mathbf{A}}$ at some rational $q_i \in \mathcal{Q}^{\mathbf{A}} \cap]a_i, a_{i+1}[\cap \mathbb{Q}$.

If $V(\mathbf{F}) \cap \mathbb{R}^n$ is empty then so are the varieties $V\left(\mathsf{ListSamplePoints}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ and $V\left(\mathsf{ListCriticalPoints}^{\mathbf{A}}\right) \cap \mathbb{R}^n$. Since $V(\mathbf{F}) \cap \mathbb{R}^n$ is empty, each call to the routine IsEmpty in the loop returns false. Hence, the algorithm leaves the loop without returning any value, so that $a_{k+1} = +\infty$ is returned.

Finally, this proves that the routine FindInfimum is correct. □

5. Proof of Theorem 4.1. This section is devoted to prove Theorem 4.1 that we restate below.

Let $f \in \mathbb{Q}[\mathbf{X}]$ *and* $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ *satisfying assumptions* $\mathbf{R}$. *There exists a non-empty Zariski open set* $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ *such that for all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, *the properties* $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ *and* $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ *hold.*

Actually, we prove that Property $\mathfrak{R}(f, \mathbf{F})$ is always true if $\mathbf{F}$ satisfies assumptions $\mathbf{R}$. Next, we prove that there exists a non-empty Zariski open set $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that for any $\mathbf{A}\mathscr{O}_1$, Property $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds. Likewise, we prove that there exists a non-empty Zariski open set $\mathscr{O}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that for any $\mathbf{A} \in \mathscr{O}_2$, Property $\mathfrak{P}_2(f, \mathbf{F})$ is satisfied. Then for any $\mathbf{A}$ in the non-empty Zariski open set $\mathscr{O} = \mathscr{O}_1 \cap \mathscr{O}_2$, the three properties $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold.

The first two results are minor generalizations of [33, Lemma 2.2] and [33, Lemma 2.3], where V is assumed to be smooth. The proofs of these lemmas in [33] can be extended mutatis mutandis to our case by noticing that x is a singular point of $V(\mathbf{F}, f - t)$ if and only it is a singular point of V or a point such that $t = f(x)$ is a critical value of $f_{|V}$.

PROPOSITION 5.1. *[33, Lemma 2.2] If* $\mathbf{F}$ *satisfies assumptions* $\mathbf{R}$ *then* $\mathfrak{R}(f, \mathbf{F})$ *holds.*

PROPOSITION 5.2. *[33, Lemma 2.3] There exists a non-empty Zariski open set* $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ *such that for all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ *holds.*

Finally, we prove the following.

PROPOSITION 5.3. *There exists a non-empty Zariski open set $\mathscr{O}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$, $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds.*

We recall the first two points in [32, Theorem 3, pp 134]:

THEOREM 5.4. *Let $V \subset \mathbb{C}^n$ be an algebraic variety of dimension d. There exists a non-empty Zariski open set $\mathscr{O}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$, and $1 \leq i \leq d+1$, there exist algebraic sets $V^{\mathbf{A}}_{n-i+1} \subset V^{\mathbf{A}}$ such that for all connected component $C^{\mathbf{A}}$ of $V^{\mathbf{A}} \cap \mathbb{R}^n$,*

(i) the restriction of $\pi_{\leq i-1}$ to $V^{\mathbf{A}}_{n-i+1}$ is proper;

(ii) the boundary of $\pi_{\leq i}\left(C^{\mathbf{A}}\right)$ is contained in $\pi_{\leq i}\left(C^{\mathbf{A}} \cap V^{\mathbf{A}}_{n-i+1}\right)$.

Then we state some notations about infinitesimals and Puiseux series. We denote by $\mathbb{R}\langle\varepsilon\rangle$ the real closed field of algebraic Puiseux series with coefficients in $\mathbb{R}$, where ε is an infinitesimal. We use the classical notions of bounded elements in $\mathbb{R}\langle\varepsilon\rangle^n$ over $\mathbb{R}^n$ and their limits. The limit of a bounded element $z \in \mathbb{R}\langle\varepsilon\rangle^n$ is denoted by $\lim_0(z)$. The ring homomorphism $\lim_0$ is also used on sets of $\mathbb{R}\langle\varepsilon\rangle^n$. For semi-algebraic sets $S \subset \mathbb{R}^n$ defined by a system of polynomial equations, we denote by $\mathsf{ext}(S)$ the solution set of the considered system in $\mathbb{R}\langle\varepsilon\rangle^n$. We refer to [9, Chapter 2.6] for precise statements of these notions. We can now prove Proposition 5.3.

Proof. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$ and c be a critical value of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ not isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$. We prove that there exists $x_c \in \mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}(x_c) = c$. Let $C^{\mathbf{A}}$ be a connected component of $V\left(f^{\mathbf{A}} - c\right) \cap V^{\mathbf{A}} \cap \mathbb{R}^n$.

Consider the largest $i \in \{1, \ldots, d\}$ such that $C^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right) \neq \varnothing$ while $C^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i}\right) = \varnothing$.

Let φ_i be the projection

$$\begin{array}{rccc} \varphi_i : & \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ & (x_1, \ldots, x_n) & \longmapsto & x_i \end{array} .$$

Then $\varphi_i\left(C^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right)\right) \subset \mathbb{R} - \{0\}$ is a strict subset of $\mathbb{R}$. Moreover, it is closed because of (i) and (ii) in Theorem 5.4. Then every extremum of the projection φ_i is reached. Since $\varphi_i\left(C^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right)\right) \neq \mathbb{R}$, there exists at least either a minimizer or a maximizer of φ_i. Without loss of generality, we assume that it is a local minimizer, denoted by $x^\star$.

Since c is not an isolated point in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, the set

$$\left(V\left(f^{\mathbf{A}} - c - \varepsilon\right) \cup V\left(f^{\mathbf{A}} - c + \varepsilon\right)\right) \cap V^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right) \cap \mathbb{R}^n$$

is nonempty. Then by [64, Lemma 3.6], the following sets coincide:

- $V\left(f^{\mathbf{A}} - c\right) \cap V^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right) \cap \mathbb{R}^n$
- $\lim_0\left(V\left(f^{\mathbf{A}} - c \pm \varepsilon\right) \cap V^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right)\right) \cap \mathbb{R}^n$

Then, there exists a connected component $C^{\mathbf{A}}_\varepsilon \subset \mathbb{R}\langle\varepsilon\rangle^n$ of

$$V\left(f^{\mathbf{A}} - c \pm \varepsilon\right) \cap V^{\mathbf{A}} \cap V\left(\mathbf{X}_{\leq i-1}\right) \cap \mathbb{R}\langle\varepsilon\rangle^n$$

such that $C^{\mathbf{A}}_\varepsilon$ contains a point x_ε such that $\lim_0(x_\varepsilon) = x^\star$. Moreover, we can assume that x_ε minimize the projection φ_i over $C^{\mathbf{A}}_\varepsilon$. Indeed, in the converse, there exists $x'_\varepsilon \in C^{\mathbf{A}}_\varepsilon$ such that $\varphi_i(x'_\varepsilon) < \varphi_i(x_\varepsilon)$, that implies $\lim_0 \varphi_i(x'_\varepsilon) \leq \varphi_i(x^\star)$. Since $x^\star$ is a minimizer, this implies that $\lim_0 \varphi_i(x'_\varepsilon) = \varphi_i(x^\star)$ and we replace x_ε with x'_ε (note that $\lim_0(x'_\varepsilon)$ is not necessarily $x^\star$ but its image by φ_i is the same as $\varphi_i(x^\star)$).

As a minimizer of the projection, x_ε lies in the algebraic set defined as the vanishing set of

- the polynomials in $\mathbf{F}^{\mathbf{A}}$,
- the minors of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}}-c\pm\varepsilon,\mathbf{F}^{\mathbf{A}}\right],i+1\right)$,
- and the variables $X_1,\ldots,X_{i-1}$.

Since $\mathsf{Jac}\left(\left[f^{\mathbf{A}}-c\pm\varepsilon,\mathbf{F}^{\mathbf{A}}\right],i+1\right)=\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right],i+1\right)$, this algebraic set is exactly $\mathsf{ext}\left(\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right)$. Furthermore, since ε is an infinitesimal, $c\pm\varepsilon$ is not a critical value of $f^{\mathbf{A}}$. Then $x_\varepsilon\notin\mathsf{ext}\left(\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)\right)$. This means that $x^\star$ is the limit of a sequence that lies in $\mathsf{ext}\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\right)$. Hence $x^\star=\lim_0 x_\varepsilon$ lies in $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. Moreover since $f^{\mathbf{A}}(x^\star)=c$ that is a local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}}\cap\mathbb{R}^n}$, $x^\star\in\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. In other words,

$$x^\star\in\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\cap\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)=\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right),$$

that concludes the proof. □

Finally, Theorem 4.1 is true with $\mathscr{O}=\mathscr{O}_1\cap\mathscr{O}_2$. Since $\mathscr{O}_1$ and $\mathscr{O}_2$ are non-empty Zariski open sets, $\mathscr{O}$ is also a non-empty Zariski open set.

6. Complexity analysis.

6.1. Geometric degree bounds. In this section, we assume that the polynomial f and the polynomials f_i have degree $\leq D$. Recall that the degree of an irreducible algebraic variety $V\subset\mathbb{C}^n$ is defined as the maximum finite cardinal of $V\cap L$ for every linear subspace $L\subset\mathbb{C}^n$. If V is not irreducible, $\deg V$ is defined as the sum of the degrees of its irreducible components. The degree of a hypersurface $V(f)$ is bounded by $\deg f$. Given a variety $V=V(g_1,\ldots,g_p)$, we denote by $\delta(V)$ the maximum of the degrees $\deg\left(V(g_1,\ldots,g_i)\right)$, for $1\leq i\leq p$. Our goal in this section is to estimate the degree of the geometric objects computed in the algorithm. Obtaining such estimations is relevant since the complexity of the algorithm relies on these degrees.

Proposition 6.1. *For all $\mathbf{A}\in\mathrm{GL}_n(\mathbb{Q})\cap\mathscr{O}$, for $1\leq i\leq d$, $\delta\left(\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right)$ and $\delta\left(\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right)$ are bounded by $D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}$.*

Proof. Let $E_1=V\left(f^{\mathbf{A}}-T,\mathbf{F}^{\mathbf{A}}\right)$ and denote by $E_2,E_3,\ldots,E_p$ the zero-sets of each minor of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right],i+1\right)$. Then for $2\leq j\leq p$, each E_j has degree bounded by $(n-d+1)(D-1)$. Moreover, it is straightforward to see that E_1 has degree bounded by D^{n-d} and dimension d. Let $1\leq k\leq p$. Then using [37, Proposition 2.3] we get

$$\deg\left(\bigcap_{1\leq j\leq k}E_j\right)\leq\deg E_1\left(\max_{1<j\leq k}\deg E_j\right)^{\dim E_1}. \tag{6.1}$$

In particular,

$$\deg\left(\bigcap_{1\leq j\leq k}E_j\right)\leq D^{n-d}\left((n-d+1)(D-1)\right)^d.$$

By Bézout's inequality ([37, Proposition 2.3]), it follows that the degree of $\bigcap_{1\leq j\leq k}E_j\cap V\left(\mathbf{X}_{\leq i-1}\right)$ is also bounded by $D^{n-d}\left((n-d+1)(D-1)\right)^d$. Finally, this implies that

$$\delta\left(\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right)\leq D^{n-d}\left((n-d+1)(D-1)\right)^d. \tag{6.2}$$

It remains to prove that $\delta\left(\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right) \leq D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}$. From the above inequality (6.2), we deduce that

$$\delta\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\right) \leq D^{n-d}\left((n-d+1)(D-1)\right)^{d}.$$

Finally, we apply [37, Proposition 2.3] with the varieties $F_1,\ldots,F_t$, where

$$F_1 = \overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$$

and $F_2,F_3,\ldots,F_t$ are the zero-sets of each minor defining $\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. Since these minors have degree bounded by $(n-d+1)(D-1)$, this quantity bounds the degree of the hypersurfaces they define. By Proposition 4.4, $F_1 = \overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension 1. Then inequality (6.1) becomes

$$\deg\left(\bigcap_{1\leq j\leq t} F_j\right) \leq D^{n-d}\left((n-d+1)(D-1)\right)^{d} \times (n-d+1)(D-1).$$

We conclude that

$$\delta\left(\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right) \leq D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}.$$

□

6.2. Complexity estimates. Let $\mathbf{A}\in \mathrm{GL}_n(\mathbb{Q})\cap\mathscr{O}$. Let $\mathbf{F}=\{f_1,\ldots,f_s\}\subset \mathbb{Q}[\mathbf{X}]$, f and g in $\mathbb{Q}[\mathbf{X}]$ of degree bounded by D that are given by a straight-line program (SLP) of size $\leq L$. Recall that d denotes the dimension of $V=V(\mathbf{F})$.

To estimate the complexity of our algorithm, we use the the geometric resolution algorithm [31, 52] and its subroutines. This is a probabilistic algorithm for polynomial system solving. In the sequel, a geometric resolution is a representation of a variety by a parametrization. A lifting fiber is a data from which a geometric resolution can be recovered. We refer to [31, 52, 73] for precise statements.

We describe the geometric resolution probabilistic subroutines and their complexity used to represent the varieties in our algorithm in Section 6.2.1. The complexity depends on the geometric degree and the maximal size of the SLPs representing the polynomials involved in the definition of our varieties. Then Section 6.2.2 is devoted to give bounds on the size of these SLPs. Then estimations of the complexity of our subroutines and the main algorithm are given in the rest of this Section.

6.2.1. Geometric Resolution subroutines.

- GeometricSolveRRS [31, Section 7]: let $\mathbf{F}=\{f_1,\ldots,f_n\}$ and g be polynomials in $\mathbb{Q}[\mathbf{X}]$ of degree $\leq D$ and given by a straight-line program of length E. Assume that $\mathbf{F}$ defines a *reduced regular sequence* in the open subset $\{g\neq 0\}$. This routine returns a geometric resolution of $\overline{V(\mathbf{F})\setminus V(g)}^{\mathcal{Z}}$ in probabilistic time
$$\widetilde{O}\left(\left(nE+n^4\right)\left(D\delta\left(V(\mathbf{F})\right)\right)^2\right).$$
- GeometricSolve [52, Section 5.2]: let $\mathbf{F}$ and g be as above of degree $\leq D$ given by a straight-line program of length E. This routine returns an equidimensional decomposition of $\overline{V(\mathbf{F})\setminus V(g)}^{\mathcal{Z}}$, encoded by a set of irreducible lifting fibers in probabilistic time
$$\widetilde{O}\left(sn^4\left(nE+n^4\right)\left(D\delta\left(V(\mathbf{F})\right)\right)^3\right).$$

- SplitFiber [52, Section 3.4]: given a lifting fiber F of a variety $V(\mathbf{F})$, it returns a set of irreducible lifting fibers of $V(\mathbf{F})$ in time

$$\widetilde{O}\left(sn^4\left(nE+n^4\right)\left(D\delta\left(V\left(\mathbf{F}\right)\right)\right)^3\right).$$

- LiftCurve [52, Section 3.3]: given an irreducible lifting fiber F of the above output, this routine returns a rational parametrization of the lifted curve of F in time

$$\widetilde{O}\left(sn^4\left(nE+n^4\right)\left(D\delta\left(V\left(\mathbf{F}\right)\right)\right)^2\right).$$

- OneDimensionalIntersect [31, Section 6]: let $\mathbf{F}$ be as above such that $\langle\mathbf{F}\rangle$ is a 1-dimensional ideal, $\mathfrak{I}$ be a geometric resolution of $\langle\mathbf{F}\rangle$, and f and g be polynomials. In case of success, the routine returns a rational parametrization of $\overline{V\left(\mathfrak{I}+f\right)\cap V\left(g\right)}^{\mathcal{Z}}$ in time

$$\widetilde{O}\left(n\left(E+n^2\right)\left(D\delta\left(V\left(\mathbf{F}\right)\right)^2\right)\right).$$

- LiftParameter [73, Section 4.2]: let T be a parameter and let $\mathcal{P}_T$ be a set of polynomials in $\mathbb{Q}(T)[X_1,\ldots,X_n]$ be given by a straight-line program of length E. Let $t\in\mathbb{R}$ be a generic point and $\mathcal{P}_t$ be the polynomial system specialized at t. If $V(\mathcal{P}_t)$ is 0-dimensional, the routine takes as input a geometric resolution of $\mathcal{P}_t$ and returns a parametric geometric resolution of $\mathcal{P}_t$ in time

$$\widetilde{O}\left(\left(nE+n^4+n\right)\delta\left(V\left(\mathcal{P}_t\right)\right)\left(4\delta\left(V\left(\mathcal{P}_T\right)\right)+1\right)\right).$$

- Difference [52, Section 4.1]: let V_1, V_2 be algebraic varieties defined as the vanishing set of polynomial families given by a straight line program of length E and represented by lifting fibers. In case of success, the routine returns a fiber F of the components of $\overline{V_1\setminus V_2}^{\mathcal{Z}}$ in time

$$\widetilde{O}\left(n^4\left(nE+n^4\right)\delta\left(V_2\right)^2\delta\left(V_1\right)\right).$$

6.2.2. Size of SLP. We want to estimate some parameters depending on the inputs of the geometric resolution routines, that are the polynomials defining the varieties $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ and $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$. Since bounds on $\delta\left(\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right)$ and $\delta\left(\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\right)$ have been obtained in the previous section, it remains to estimates the size of the straight-line programs representing these polynomials. These polynomials are either a polynomial $f^{\mathbf{A}}$ or $f_i^{\mathbf{A}}$ or a minor of size $n-d+1$ of the Jacobian matrix $\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right],i+1\right)$. The polynomials f and f_i are given as a SLP of size L. Then $f^{\mathbf{A}}$ and $f_i^{\mathbf{A}}$, can be represented by a SLP of size $O\left(L+n^2\right)$. Then we estimate the size of the minors. Let ω be the matrix-multiplication exponent.

PROPOSITION 6.2. *Each minors of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right],i+1\right)$ can be represented by a SLP of size $\widetilde{O}\left(\left(n-d+1\right)^{\omega/2+2}\left(L+n^2\right)\right)$.*

Proof. The partial derivatives appearing in the Jacobian matrix come from $f^{\mathbf{A}}$ and $f_i^{\mathbf{A}}$, represented by a SLP of size $O\left(L+n^2\right)$. According to [10], each partial derivative $\frac{\partial f_i^{\mathbf{A}}}{\partial x_j}$ and $\frac{\partial f^{\mathbf{A}}}{\partial x_j}$ can be represented by a SLP of size $O\left(L+n^2\right)$. Moreover,

according to [45], the determinant of an $n \times n$ matrix can be computed using only $+$, $-$ and $\times$ in $\widetilde{O}\left((n-d+1)^{\omega/2+2}\right)$ operations. We combine these two results to conclude the proof. □

REMARK 6.3. *Recall that $\omega \leq 3$. In the sequel, to lighten the expressions of complexity, we replace the above complexity $\widetilde{O}\left((n-d+1)^{\omega/2+2}\left(L+n^2\right)\right)$ with $\widetilde{O}\left(n^4\left(L+n^2\right)\right)$, that is less accurate but that dominates the first one.*

6.2.3. Computation of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. Recall that the algebraic variety $\mathscr{C}\left(f^{\mathbf{A}},F^{\mathbf{A}},i\right)$ is defined as the vanishing set of

- the polynomials $f_1^{\mathbf{A}},\ldots,f_s^{\mathbf{A}}$,
- the minors of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right],i+1\right)$,
- and the variables $X_1,\ldots,X_{i-1}$.

The algebraic set $\mathscr{C}\left(f^{\mathbf{A}},F^{\mathbf{A}},i\right)$ can be computed by $\mathsf{GeometricSolve}$ called with $s+\binom{s+1}{n-d+1}\binom{n-i}{n-d+1}=O\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)$ polynomials in n variables. Each polynomial is given by a SLP of size $\widetilde{O}\left(n^4\left(L+n^2\right)\right)$. Hence, the input system is represented by a SLP of size E in $\widetilde{O}\left(\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)n^4\left(L+n^2\right)\right)$. By Proposition 6.1, $\delta\left(\mathscr{C}\left(f^{\mathbf{A}},F^{\mathbf{A}},i\right)\right)$ is bounded by $D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}$. Hence, the computation can be done within

$$\widetilde{O}\left(s\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$$

arithmetic operations in $\mathbb{Q}$. Since $\binom{n}{n-d+1}\leq 2^n$, this complexity is bounded by $\widetilde{O}\left(\left(s^2+s2^n\binom{s+1}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$.

Likewise, $\mathsf{Crit}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)$ is defined as the vanishing set of

- the polynomials $f_1^{\mathbf{A}},\ldots,f_s^{\mathbf{A}}$,
- the minors of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right]\right)$.

Hence, the complexity of its computation by $\mathsf{GeometricSolve}$ is the same as the above complexity of the computation of $\mathscr{C}\left(f^{\mathbf{A}},F^{\mathbf{A}},i\right)$.

The computation of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ is done using $\mathsf{Difference}$. Its complexity is in $\widetilde{O}\left(ED^{3(n-d)}\left((n-d+1)(D-1)\right)^{(d+1)}\right)$. It is dominated by the cost of the computation of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$, thus we get the following complexity result.

LEMMA 6.4. *There exists a probabilistic algorithm that takes as input $f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}$ and i and returns an equidimensional decomposition of $\overline{\mathscr{C}\left(f^{\mathbf{A}},F^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$, encoded by a lifting fiber. In case of success, the algorithm has a complexity dominated by $\widetilde{O}\left(\left(s^2+s2^n\binom{s+1}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$.*

6.2.4. Computation of $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$. Since $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ is defined as the intersection $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\cap \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$, a geometric resolution of each component of $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ is obtained from a set of irreducible lifting fibers of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. From the output of the algorithm presented in Section 6.2.3, a set of irreducible lifting fibers is recovered using $\mathsf{SplitFiber}$ in time $\widetilde{O}\left(sED^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$. As in Section 6.2.3, the size E is in $\widetilde{O}\left(\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)n^4\left(L+n^2\right)\right)$. The routine $\mathsf{LiftCurve}$ is used on each irre-

ducible fiber in order to obtain a parametrization of each component of the curve $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. Lifting one fiber is done in

$$\widetilde{O}\left(s\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)LD^{2(n-d+1)}\left((n-d+1)(D-1)\right)^{2(d+1)}\right).$$

From such a parametrization, the routine OneDimensionalIntersect is used with every polynomial that defines $\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. There are $\binom{s+1}{n-d+1}\binom{n}{n-d+1}$ such polynomials, thus the cost to compute the rational parametrization corresponding to one irreducible fiber is at most

$$\widetilde{O}\left(\binom{s+1}{n-d+1}\binom{n}{n-d+1}LD^{2(n-d+1)}\left((n-d+1)(D-1)\right)^{2(d+1)}\right).$$

The total cost for the $D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}$ irreducible lifting fibers is dominated by $\widetilde{O}\left(s\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$. Finally, we compute a parametrization of the union of the zero-sets of the previous parametrization using [71, Lemma 9.1.3]. Since the sum of the degrees of each parametrization is bounded by $D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}$, the cost is negligible. Since $\binom{n}{n-d+1}\leq 2^n$, we get the following result.

LEMMA 6.5. *There exists a probabilistic algorithm that takes as input a set of lifting fibers of* $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ *and that returns a rational parametrization of* $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$. *In case of success, the algorithm has a complexity dominated by* $\widetilde{O}\left(\left(s^2+s2^n\binom{s+1}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$.

6.2.5. Complexity of SetOfNonProperness. As explained in [66, Section 4], the computation of the set of non-properness of the restriction of the projection π_T to $V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\times\mathbb{C}\right)$ from the representation of the variety $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ can be done using a parametric geometric resolution [73]. Indeed, from a set of lifting fibers of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$, obtained by the routine GeometricSolve, one can compute a geometric resolution of $V\left(f^{\mathbf{A}}-t\right)\cap\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ for a generic $t\in\mathbb{R}$. Since there are at most $D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}$ lifting fibers, it is done using OneDimensionalIntersect on all the fibers in $\widetilde{O}\left(ED^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$, where as in Section 6.2.3, E is in $\widetilde{O}\left(\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)n^4\left(L+n^2\right)\right)$.

From these geometric resolutions, LiftParameter computes a parametric geometric resolution $(q,q_0,\ldots,q_n)$ of $V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\times\mathbb{C}\right)$, where T is a parameter, in $\widetilde{O}\left(ED^{3(n-d)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$. As explained in [66, Section 4], the set of non-properness is contained in the roots of the least common multiple of the denominators of the coefficients of the polynomial q. Since $\binom{n}{n-d+1}\leq 2^n$, we get the following result.

LEMMA 6.6. *There exists a probabilistic algorithm that takes as input a set of lifting fibers of* $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ *and that returns a polynomial whose set of roots contains the set of non-properness of the projection* π_T *restricted to* $V\left(f^{\mathbf{A}}-T\right)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus \mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\times\mathbb{C}\right)$. *In case of success, the algorithm has a com-*

plexity dominated by $\widetilde{O}\left(\left(s^2+s2^n\binom{s+1}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$.

6.2.6. Complexity of RealSamplePoints **and** IsEmpty**.** Given $\mathbf{F}=\{f_1,\ldots,f_s\}$, an algorithm computing a set of real sample points of $V(\mathbf{F})\cap\mathbb{R}^n$ is given in [68]. It relies on the computation of polar varieties. Using techniques described in [5, 4, 71] and [7, Section 3], a local description of the polar varieties as a complete intersection can be obtained. Assume that $V(\mathbf{F})$ is equidimensional of dimension d. Such a local description depends on the choice of a minor of size $n-d$ of the Jacobian matrix $\mathsf{Jac}(\mathbf{F})$. Since there are $\binom{s}{n-d}\binom{n}{n-d}$ minors of size $n-d$ in $\mathsf{Jac}(\mathbf{F})$, a full description of the polar varieties is obtained by computing the $\binom{s}{n-d}\binom{n}{n-d}$ possible localizations. Each local description is given by a reduced regular sequence involving $n-d$ polynomials in $\mathbf{F}$ and minors of degree bounded by $(n-d+1)(D-1)$. Hence, the routine GeometricSolveRRS computes one local description in $\widetilde{O}\left(LD^{2(n-d+1)}\left((n-d+1)(D-1)\right)^{2(d+1)}\right)$ so the cost for all localizations is in $\widetilde{O}\left(\binom{s}{n-d}\binom{n}{n-d}LD^{2(n-d+1)}\left((n-d+1)(D-1)\right)^{2(d+1)}\right)$. Note that in [68], the complexity is cubic instead of quadratic in the geometric degree of the inputs because these localization techniques are not used to estimate the complexity.

Since $\binom{n}{n-d}\leq 2^n$, this leads to the following complexity result.

LEMMA 6.7. *There exists a probabilistic algorithm that takes as input* $\mathbf{F}$ *satisfying assumptions* $\mathbf{R}$ *and that returns a set of real sample points of* $V(F)\cap\mathbb{R}^n$*, encoded by a rational parametrization. In case of success, the algorithm has a complexity dominated by* $\widetilde{O}\left(2^n\binom{s}{n-d}LD^{2(n-d+1)}\left((n-d+1)(D-1)\right)^{2(d+1)}\right)$.

6.2.7. Complexity of SetContainingLocalExtrema**.** The first step in SetContainingLocalExtrema is the computation of a set of real sample points of $V\left(\mathbf{F}^{\mathbf{A}}\right)\cap\mathbb{R}^n$. Its complexity is given in Lemma 6.7. Then at the i-th step of the loop, $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$, the set of non-properness of the projection π_T restricted to $V(f-T)\cap\left(\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathsf{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\times\mathbb{C}\right)$ and $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ are computed. The costs are given in Lemma 6.4, Lemma 6.6 and Lemma 6.5. The complexity for one step is in $\widetilde{O}\left(\left(s^2+s2^n\binom{s+1}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$. Finally, for the d steps, since $d\leq n$ can be omitted, we get the following complexity.

LEMMA 6.8. *In case of success, the routine* SetContainingLocalExtrema *performs at most* $\widetilde{O}\left(\left(s^2+s2^n\binom{s+1}{n-d+1}\right)LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$ *arithmetic operations in* $\mathbb{Q}$.

6.2.8. Complexity of FindInfimum**.** The most expensive steps in this routine are the calls to IsEmpty. There are at most k such steps, where k is the number of points of non-properness, of critical values and of real sample points. Using the Bézout inequality, k lies in $\widetilde{O}\left(D^{n-d}\left((n-d+1)(D-1)\right)^{d+1}\right)$. Using the complexity estimate given in Lemma 6.7, this leads to the following.

LEMMA 6.9. *In case of success, the routine* FindInfimum *performs at most*

$$\widetilde{O}\left(2^n\binom{s}{n-d}LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right).$$

6.2.9. Complexity of the Algorithm. Finally, the complexity of Optimize comes from Lemma 6.8 and Lemma 6.9, using that $\binom{s}{n-d} \leq \binom{s+1}{n-d+1}$.

THEOREM 6.10. *In case of success, the algorithm* Optimize *performs*

$$\widetilde{O}\left(\left(s^2 + s2^n\binom{s+1}{n-d+1}\right) LD^{3(n-d+1)}\left((n-d+1)(D-1)\right)^{3(d+1)}\right)$$

arithmetic operations in $\mathbb{Q}$.

Remark that if $\mathbf{F}$ is a reduced regular sequence then the complexity is simpler.

THEOREM 6.11. *If* $\mathbf{F}$ *is a reduced regular sequence, the algorithm* Optimize *performs* $\widetilde{O}\left(L\left(\sqrt[3]{2}(s+1)D\right)^{3(n+2)}\right)$ *arithmetic operations in* $\mathbb{Q}$.

7. Implementation and practical experiments. We give details about our implementation in Section 7.1. Instead of using the geometric resolution algorithm for algebraic elimination, we use Gröbner bases that still allow to perform all geometric operations needed to implement the algorithm (see [18] for an introduction to Gröbner bases). Moreover, there exist practically efficient algorithms for computing Gröbner bases [24, 25]. This way, the probabilistic aspect of our algorithm relies on the random choice of a linear change of variables. In practice, we check whether the linear change of variables is suitable. Thus one can guarantee exactness. This is explained in Section 7.1.

In Sections 7.2 and 7.3, we present practical experiments. First, we run our implementation with random dense polynomials, that is the hardest case for the inputs. As an example, our implementation can solve problems with an objective polynomial and one constraint, both of degree 2, with up to 32 variables using 4 hours of CPU time. With two constraints, our implementation can solve problems with up to 11 variables using 5.3 hours of CPU time. With a linear objective polynomial subject to one constraint of degree 4, both in 5 variables, it takes 34 minutes. These results show that our implementation outperforms general symbolic solvers based on the Cylindrical Algebraic Decomposition.

Then we run examples coming from applications. Some of these examples can be solved by QEPCAD. The timings are given in Section 7.3.

We do not report timings of methods based on sums of squares or numerical procedures, e.g. [53, 62, 39] since their outputs are numerical approximation while our algorithm provides exact outputs.

7.1. Implementation. Since our algorithm depends on the choice of a matrix that defines a change of coordinates, it is probabilistic. However, we present a technique to make sure that this choice is a correct one. This technique is used in our implementation.

As stated in Section 4, the algorithm is correct if the subroutines SetContainingLocalExtrema and FindInfimum are correct. According to Proposition 4.2, if the random matrix chosen at the first step of Optimize is such that $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold, then SetContainingLocalExtrema runs correctly. Then its output satisfies property $\mathrm{Opt}\left(W(f, \mathbf{F}), V(\mathbf{F})\right)$. Hence, FindInfimum can be called with the output of SetContainingLocalExtrema.

Then the choice of the matrix $\mathbf{A}$ leads to a correct output if $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold.

Property $\mathfrak{R}(f, \mathbf{F})$ always holds if $\mathbf{F}$ satisfies assumptions $\mathbf{R}$ (see [33, Lemma 2.2]). Since for any change of coordinates, $\mathbf{F}$ satisfies assumptions $\mathbf{R}$ if and only if $\mathbf{F}^{\mathbf{A}}$ does,

$\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds for any $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$. Then it remains to check $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$. Both properties depend on the properness of projections of the form

$$\begin{aligned} \pi_{\leq d}: \quad & W \subset \mathbb{C}^n \longrightarrow \mathbb{C}^d \\ & (x_1, \ldots, x_n) \longmapsto (x_1, \ldots, x_d) \end{aligned}$$

where W is an algebraic variety. According to [44, Proposition 3.2], if I_V is an ideal such that $V = V(I_V)$ has dimension d then the projection

$$\begin{aligned} \pi_{\leq d}: \quad & V \subset \mathbb{C}^n \longrightarrow \mathbb{C}^d \\ & (x_1, \ldots, x_n) \longmapsto (x_1, \ldots, x_d) \end{aligned}$$

is proper if and only if I_V is in Noether position.

Thus we choose the matrix $\mathbf{A}$ such that after the change of variables, the ideals are in Noether position. This can be done using techniques described in [47, Section 4.1.2] and [54]. These techniques are used in our implementation to obtain a matrix as sparse as possible that makes SetContainingLocalExtrema correct.

7.2. Practical experiments. The analysis of the degree of the algebraic varieties involved in the computations provides a singly exponential bound in the number of indeterminates. This matches the best complexity bounds for global optimization algorithms using quantifier elimination. Our implementation is written in Maple. Gröbner bases are computed using the package FGb [23] (`http://www-polsys.lip6.fr/~jcf/Software/`.)

The computations were performed on a Intel Xeon CPU E7540 @ 2.00GHz and 250GB of RAM.

In the tables below, we use the following notations:

- d: degree of the objective polynomial f;
- D: upper bound for the degree of the constraints;
- n: number of indeterminates;
- s: number of constraints;
- obj terms: number of terms in the objective polynomial;
- terms: average number of terms.

To test the behavior of the algorithm, we run it with randomly generated polynomials and constraints as inputs.

Considering an objective polynomial and one constraint, both of degree 2 and increasing the number of variables, our implementation can solve problems with up to 32 variables in 4 hours. For this special case, the algorithm seems to be sub-exponential.

Constraints of degree 2.

n	d	D	s	obj terms	terms	time
8	2	2	1	44	45	9 sec.
12	2	2	1	91	91	30 sec.
16	2	2	1	153	153	2 min..
20	2	2	1	229	231	8 min.
24	2	2	1	323	323	27 min.
28	2	2	1	433	433	1.5 hours
32	2	2	1	559	557	4 hours
7	2	2	2	36	36	92 sec.
8	2	2	2	45	45	7 min.
9	2	2	2	55	55	27 min.
10	2	2	2	65	66	1.6 hours
11	2	2	2	78	78	5.3 hours

Constraints of degree 3.

n	d	D	s	obj terms	terms	time
4	2	3	1	15	34	4 sec.
5	2	3	1	21	55	28 sec.
6	2	3	1	27	84	9 min.
7	2	3	1	36	120	3.5 hours
4	2	3	2	15	34	81 sec.
5	2	3	2	21	56	2.2 hours

Constraints of degree 4.

n	d	D	s	obj terms	terms	time
2	3	4	1	10	14	2 sec.
3	3	4	1	20	34	4 sec.
4	3	4	1	34	70	7 min.
3	3	4	2	20	35	22 sec.
4	3	4	2	35	70	4.8 hours.
2	2	4	1	6	15	1 sec.
3	2	4	1	10	35	2 sec.
4	2	4	1	15	68	83 sec.

Linear objective function.

n	d	D	s	obj terms	terms	time
4	1	3	1	5	34	3 sec.
4	1	4	1	5	69	30 sec.
4	1	5	1	5	126	13 min.
5	1	3	1	6	56	7 sec.
5	1	4	1	6	126	34 min.
5	1	5	1	6	252	87 hours
6	1	3	1	7	84	68 sec.
6	1	4	1	7	207	62 hours
4	1	3	2	5	35	36 sec.
4	1	4	2	5	70	1 hour
4	1	5	2	5	126	33 hours

7.3. Examples coming from applications. We consider examples coming from applications to compare the execution time of our algorithm with a cylindrical algebraic decomposition algorithm. These decompositions are computed using QEPCAD version B 1.69[1] These examples are described in Appendix A and available as a plain text file openable with Maple at `http://www-polsys.lip6.fr/~greuet/`.

	n	d	D	s	obj terms	terms	time	QEPCAD
nonreached	3	4	1	1	4	1	2.3 sec.	0.03 sec.
nonreached2	3	10	3	1	5	5	2 sec.	∞
isolated	2	4	3	1	2	2	0.8 sec.	0.04 sec.
reachedasymp	3	14	1	1	3	1	1 sec.	7.3 sec.
GGSZ2012	2	2	3	1	2	2	0.6 sec.	10.5 sec.
Nie2010	3	6	1	1	7	4	1.3 sec.	∞
LaxLax	4	4	1	3	5	2	0.6 sec.	∞
maxcut5-1	5	2	2	5	11	2	0.3 sec.	∞
maxcut5-2	5	2	2	5	11	2	0.3 sec.	∞
Coleman5	8	2	2	4	8	4	5 sec.	∞
Coleman6	10	2	2	5	10	4	33 sec.	∞
Vor1	6	8	n/a	0	63	n/a	2 min.	∞

[1]Implementation originally due to H. Hong, and subsequently added on to by C. W. Brown, G. E. Collins, M. J. Encarnacion, J. R. Johnson, W. Krandick, S. McCallum, S. Steinberg, R. Liska, N. Robidoux. Latest version is available at `http://www.usna.edu/cs/~qepcad/`.

Appendix A. Description of examples.

EXAMPLE 1 (nonreached, nonreached2). Let $g(x_1, x_2, x_3) = x_1^2 - x_1x_2 + x_1x_2x_3 + x_2 + 3$ and consider the two problems

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & (x_1x_2 - 1)^2 + x_2^2 + x_3^2 + 42 \\ \text{s.t.} & x_3 = 0. \end{cases}$$

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & (x_1x_2 - 1)^2 + x_2^2 + x_3^2 g + (x_1 + 1)\, g^3 + 42 \\ \text{s.t.} & g(x_1, x_2, x_3) = 0. \end{cases}$$

Their infima are not reached. They are the limit of sequences $f(z_k)$, where $\|z_k\|$ tends to infinity. For instance, z_k can be of the form $\left(x_1^{(k)}, \frac{1}{x_1^{(k)}}, x_3^{(k)}\right)$, where $x_1^{(k)}$ tends to infinity. Note that both examples cause instabilities to numerical algorithms.

EXAMPLE 2 (isolated). It is a toy example: $f^\star$ is isolated in $f(V \cap \mathbb{R}^n)$.

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^2} & \left(x_1^2 + x_2^2 - 2\right)\left(x_1^2 + x_2^2\right) \\ \text{s.t.} & \left(x_1^2 + x_2^2 - 1\right)(x_1 - 3) = 0. \end{cases}$$

On $V \cap \mathbb{R}^n$, either $x_1^2 + x_2^2 = 1$ or $x_1 = 3$. Then the objective polynomial is either equal to -1 or $\left(7 + x_2^2\right)\left(9 + x_2^2\right)$. The second expression is positive over the reals.

EXAMPLE 3 (reachedasympt). The infimum is both attained and an asymptotic value. Indeed, $f^\star = 42$ is reached at any point $(x_1, 0, 0)$, but is also the limit of sequences of the form $\left(x_1, \frac{1}{x_1}, 0\right)$ when x_1 tends to infinity. Some iterative methods do not return a minimizer close to $(x_1, 0, 0)$.

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & \left(10000\,(x_1x_2 - 1)^4 + x_1^6\right) x_2^6 + \frac{1}{124}x_3^2 + 42 \\ \text{s.t.} & x_3 = 0. \end{cases}$$

EXAMPLE 4 (GGSZ2012). It comes from [33] (Example 4.4). The minimizer does not satisfy the KKT conditions.

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^2} & (x_1 + 1)^2 + x_2^2 \\ \text{s.t.} & x_1^3 = x_2^2. \end{cases}$$

EXAMPLE 5 (Nie2011). It comes from [58] (Example 5.2). It has been studied in [33] because of the numerical instabilities that occurs with numerical algorithms.

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & x_1^6 + x_2^6 + x_3^6 + 3x_1^2x_2^2x_3^2 - x_1^2(x_2^4 + x_3^4) - x_2^2(x_3^4 + x_1^4) - x_3^2(x_1^4 + x_2^4) \\ \text{s.t.} & x_1 + x_2 + x_3 - 1 = 0. \end{cases}$$

EXAMPLE 6 (LaxLax). The objective polynomial appears in [50] and [46]. Its infimum is 0 and is reached over $V(x_1, x_2 - x_3, x_3 - x_4) \cap \mathbb{R}^n$.

$$\begin{cases} \inf\limits_{(x)\in\mathbb{R}^4} & x_1x_2x_3x_4 - x_1(x_2 - x_1)(x_3 - x_1)(x_4 - x_1) \\ & -x_2(x_1 - x_2)(x_3 - x_2)(x_4 - x_2) - x_3(x_1 - x_3)(x_2 - x_3)(x_4 - x_3) \\ & -x_4(x_1 - x_4)(x_2 - x_4)(x_3 - x_4) \\ \text{s.t.} & x_1 = x_2 - x_3 = x_3 - x_4 = 0. \end{cases}$$

EXAMPLE 7 (maxcut5-1/5-2). A cut of a graph with weighted edges is a partition of the vertices into two disjoint subsets. Its weight is the sum of the weights of the edges crossing the cut. The maxcut problem is to find a cut whose weight is greater than or equal to any other cut. This problem has applications, among other, in very-arge-scale integration circuit design and statistical physics [20, 30]. It can be reformulated has a constrained polynomial optimization problem [16]. For a graph of p vertices and weight w_{ij} for the edge joining the i-th vertex to the j-th one, it is equivalent to solve

$$\left\{\begin{array}{ll}\inf\limits_{x\in\mathbb{R}^p} & -\frac{1}{2}\sum_{1\leq i<j\leq p} w_{ij}\left(1-x_ix_j\right)\\ \text{s.t.} & x_i^2-1=0,\ \text{for } i\in\{1,\ldots,p\},\end{array}\right.$$

We use the set of weight W_{G5-1} and W_{G5-2} in [3], that leads to solve

$$\left\{\begin{array}{ll}\inf\limits_{x\in\mathbb{R}^5} & -98+\frac{23}{2}x_1x_2+8x_1x_3+9x_1x_4+\frac{17}{2}x_1x_5+\frac{25}{2}x_2x_3\\ & +13x_2x_4+\frac{23}{2}x_2x_5+7x_3x_4+12x_3x_5+5x_4x_5\\ \text{s.t.} & x_i^2-1=0,\ \text{for } i\in\{1,\ldots,5\}.\end{array}\right.$$

and

$$\left\{\begin{array}{ll}\inf\limits_{x\in\mathbb{R}^5} & -31+3x_1x_2+3x_1x_3+4x_1x_4+5x_1y_5+\frac{5}{2}x_2x_3+\frac{5}{2}x_2x_4+3x_2x_5\\ & +2x_3x_4+3x_3x_5+3x_4x_5\\ \text{s.t.} & x_i^2-1=0,\ \text{for } i\in\{1,\ldots,5\}.\end{array}\right.$$

EXAMPLE 8 (coleman5/6). They come from optimal control problems and appears in [12]. For $M\in\{5,6\}$, let $x_1,\ldots,x_{M-1}$ and $y_1,\ldots,y_{M-1}$ be the indeterminates.

$$\left\{\begin{array}{ll}\inf\limits_{(x,y)\in\mathbb{R}^{2M}} & \frac{1}{M}\sum_{i=1}^{M-1} x_i^2+y_i^2\\ \text{s.t.} & y_1-1=y_{i+1}-y_i-\frac{1}{M-1}\left(y_i^2-x_i\right)=0,\ \text{for } i\in\{1,\ldots,M-2\}.\end{array}\right.$$

EXAMPLE 9 (Vor1). It comes from [22] and have no constraints. It is too large to be written here but can be found at `http://www-polsys.lip6.fr/~greuet/`.

REFERENCES

[1] C. AHOLT, S. AGARWAL, AND R. THOMAS, *A qcqp approach to triangulation*, in Computer Vision–ECCV 2012, Springer, 2012, pp. 654–667.

[2] C. AHOLT, B. STURMFELS, AND R. THOMAS, *A hilbert scheme in computer vision*, arXiv preprint arXiv:1107.2875, (2011).

[3] B. BALASUNDARAM AND S. BUTENKO, *Constructing test functions for global optimization using continuous formulations of graph problems*, Optim. Methods Softw., 20 (2005), pp. 439–452.

[4] B. BANK, M. GIUSTI, J. HEINTZ, AND G.-M. MBAKOP, *Polar varieties and efficient real equation solving: the hypersurface case*, Journal of Complexity, 13 (1997), pp. 5–27.

[5] ———, *Polar varieties and efficient real elimination*, Mathematische Zeitschrift, 238 (2001), pp. 115–144.

[6] B. BANK, M. GIUSTI, J. HEINTZ, AND M. SAFEY EL DIN, *Intrinsic complexity estimates in polynomial optimization*, Journal of Complexity, (2014), pp. –.

[7] B. BANK, M. GIUSTI, J. HEINTZ, M. SAFEY EL DIN, AND E. SCHOST, *On the geometry of polar varieties*, Applicable Algebra in Engineering, Communication and Computing, (2010).

[8] S. Basu, R. Pollack, and M.-F. Roy, *On the combinatorial and algebraic complexity of quantifier elimination*, Journal of the ACM (JACM), 43 (1996), pp. 1002–1045.
[9] ———, *Algorithms in real algebraic geometry*, vol. 10 of Algorithms and Computation in Mathematics, Springer-Verlag, second ed., 2006.
[10] W. Baur and V. Strassen, *The complexity of partial derivatives*, Theoret. Comput. Sci., 22 (1983), pp. 317–330.
[11] C. W. Brown, *Solution formula construction for truth-invariant cads*, PhD thesis, University of Delaware, 1999.
[12] T. F. Coleman and A. P. Liao, *An efficient trust region method for unconstrained discrete-time optimal control problems*, Comput. Optim. Appl., 4 (1995), pp. 47–66.
[13] G. E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, in Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), Springer, Berlin, 1975, pp. 134–183. Lecture Notes in Comput. Sci., Vol. 33.
[14] ———, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, in Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), Springer, Berlin, 1975, pp. 134–183. Lecture Notes in Comput. Sci., Vol. 33.
[15] G. E. Collins and H. Hong, *Partial cylindrical algebraic decomposition for quantifier elimination*, in Quantifier elimination and cylindrical algebraic decomposition (Linz, 1993), Texts Monogr. Symbol. Comput., Springer, Vienna, 1998, pp. 174–200.
[16] C. W. Commander, *Maximum cut problem, max-cut*, in Encyclopedia of Optimization, Springer, 2009, pp. 1991–1999.
[17] P. Cousot, *Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming*, in Verification, Model Checking, and Abstract Interpretation, R. Cousot, ed., vol. 3385 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2005, pp. 1–24.
[18] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, 2006.
[19] J. Demmel, J. Nie, and V. Powers, *Representations of positive polynomials on noncompact semialgebraic sets via kkt ideals*, Journal of pure and applied algebra, 209 (2007), pp. 189–200.
[20] M. M. Deza and M. Laurent, *Geometry of cuts and metrics*, vol. 15 of Algorithms and Combinatorics, Springer, Heidelberg, 2010. First softcover printing of the 1997 original [MR1460488].
[21] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, 1995.
[22] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din, *The Voronoi diagram of three lines*, Discrete Comput. Geom., 42 (2009), pp. 94–130.
[23] J.-C. Faugère, *FGb*. `http://www-polsys.lip6.fr/~jcf`, .
[24] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra, 139 (1999), pp. 61–88. Effective methods in algebraic geometry (Saint-Malo, 1998).
[25] ———, *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5), in Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, New York, 2002, ACM, pp. 75–83 (electronic).
[26] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault, *Polynomial systems solving by fast linear algebra*, arXiv preprint arXiv:1304.6039, (2013).
[27] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional gröbner bases by change of ordering*, Journal of Symbolic Computation, 16 (1993), pp. 329–344.
[28] J.-C. Faugère and C. Mou, *Fast algorithm for change of ordering of zero-dimensional gröbner bases with sparse multiplication matrices*, in Proceedings of the 36th international symposium on Symbolic and algebraic computation, ACM, 2011, pp. 115–122.
[29] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer, *Critical points and gröbner bases: the unmixed case*, in Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ACM, 2012, pp. 162–169.
[30] P. Festa, P. M. Pardalos, M. G. C. Resende, and C. C. Ribeiro, *Randomized heuristics for the MAX-CUT problem*, Optim. Methods Softw., 17 (2002), pp. 1033–1058.
[31] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity, 17 (2001), pp. 154–211.
[32] A. Greuet and M. S. E. Din, *Deciding reachability of the infimum of a multivariate polynomial*, in ISSAC, 2011, pp. 131–138.
[33] A. Greuet, F. Guo, M. S. E. Din, and L. Zhi, *Global optimization of polynomials restricted to a smooth variety using sums of squares*, Journal of Symbolic Computation, 47 (2012),

pp. 503 – 518.
[34] F. Guo, M. Safey El Din, and L. Zhi, *Global optimization of polynomials using generalized critical values and sums of squares*, in Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, 2010.
[35] Q. Guo, M. Safey El Din, and L. Zhi, *Computing rational solutions of linear matrix inequalities*, in ISSAC, M. B. Monagan, G. Cooperman, and M. Giesbrecht, eds., ACM, 2013, pp. 197–204.
[36] H. V. Hà and T. S. Phạm, *Solving polynomial optimization problems via the truncated tangency variety and sums of squares*, J. Pure Appl. Algebra, 213 (2009), pp. 2167–2176.
[37] J. Heintz and C.-P. Schnorr, *Testing polynomials which are easy to compute (extended abstract)*, in STOC, 1980, pp. 262–272.
[38] D. Henrion and A. Garulli, eds., *Positive polynomials in control*, vol. 312 of Lecture Notes in Control and Information Sciences, Springer-Verlag, Berlin, 2005.
[39] D. Henrion and J.-B. Lasserre, *GloptiPoly: global optimization over polynomials with Matlab and SeDuMi*, ACM Trans. Math. Software, 29 (2003), pp. 165–194.
[40] D. Henrion, M. Šebek, and V. Kučera, *Positive polynomials and robust stabilization with fixed-order controllers*, IEEE Trans. Automat. Control, 48 (2003), pp. 1178–1186.
[41] H. Hong, *Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination*, in Papers from the international symposium on Symbolic and algebraic computation, ISSAC '92, New York, NY, USA, 1992, ACM, pp. 177–188.
[42] H. Hong and M. Safey El Din, *Variant real quantifier elimination: algorithm and application*, in Proceedings of the 2009 international symposium on Symbolic and algebraic computation, ACM, 2009, pp. 183–190.
[43] ———, *Variant quantifier elimination*, Journal of Symbolic Computation, 47 (2012), pp. 883–901.
[44] Z. Jelonek, *Testing sets for properness of polynomial mappings*, Math. Ann., 315 (1999), pp. 1–35.
[45] E. Kaltofen, *On computing determinants of matrices without divisions*, in Proc. 1992 (ISSAC'92), P. S. Wang, ed., New York, N. Y., 1992, ACM Press, pp. 342–349.
[46] E. L. Kaltofen, B. Li, Z. Yang, and L. Zhi, *Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients*, J. Symbolic Comput., 47 (2012), pp. 1–15.
[47] T. Krick, L. M. Pardo, and M. Sombra, *Sharp estimates for the arithmetic nullstellensatz*, Duke Mathematical Journal, 109 (2001), pp. 521–598.
[48] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser Boston, 1984.
[49] J.-B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim., 11 (2001), pp. 796–817 (electronic).
[50] A. Lax and P. D. Lax, *On sums of squares*, Linear Algebra and Appl., 20 (1978), pp. 71–75.
[51] D. Lazard and F. Rouillier, *Solving parametric polynomial systems*, J. Symbolic Comput., 42 (2007), pp. 636–667.
[52] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity, 19 (2003), pp. 564–596.
[53] J. Löfberg, *Yalmip: A toolbox for modeling and optimization in matlab*, Proc. IEEE CCA/ISIC/CACSD Conf., (2004).
[54] A. Logar, *A computational proof of the noether normalization lemma*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer, 1989, pp. 259–273.
[55] S. McCallum, *An improved projection operation for cylindrical algebraic decomposition*, in Quantifier elimination and cylindrical algebraic decomposition (Linz, 1993), Texts Monogr. Symbol. Comput., Springer, Vienna, 1998, pp. 242–268.
[56] D. Monniaux, *On using sums-of-squares for exact computations without strict feasibility.* , 2010.
[57] Y. Nesterov et al., *Squared functional systems and optimization problems*, High performance optimization, 33 (2000), pp. 405–440.
[58] J. Nie, *An exact jacobian SDP relaxation for polynomial optimization.* Preprint, 2011.
[59] J. Nie, J. Demmel, and B. Sturmfels, *Minimizing polynomials via sum of squares over the gradient ideal*, Math. Program., 106 (2006), pp. 587–606.
[60] P. A. Parrilo, *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*, dissertation (Ph.D.), California Institute of Technology, 2000.
[61] H. Peyrl and P. A. Parrilo, *Computing sum of squares decompositions with rational coefficients*, Theoretical Computer Science, 409 (2008), pp. 269 – 281. Symbolic-Numerical Computations.

[62] S. Prajna, A. Papachristodoulou, P. Seiler, and P. Parrilo, *Sostools: Sum of squares optimization toolbox for matlab*, (2004).
[63] F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Appl. Algebra Eng. Commun. Comput., 9 (1999), pp. 433–461.
[64] F. Rouillier, M.-F. Roy, and M. Safey El Din, *Finding at least one point in each connected component of a real algebraic set defined by a single equation*, J. Complexity, 16 (2000), pp. 716–750.
[65] F. Rouillier and P. Zimmermann, *Efficient isolation of polynomial's real roots*, in Proceedings of the International Conference on Linear Algebra and Arithmetic (Rabat, 2001), vol. 162, 2004, pp. 33–50.
[66] M. Safey El Din, *Testing sign conditions on a multivariate polynomial and applications*, Mathematics in Computer Science, 1 (2007), pp. 177–207.
[67] M. Safey El Din, *Computing the global optimum of a multivariate polynomial over the reals*, in ISSAC, 2008, pp. 71–78.
[68] M. Safey El Din and É. Schost, *Polar varieties and computation of one point in each connected component of a smooth algebraic set*, in Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, New York, 2003, ACM, pp. 224–231.
[69] ———, *Properness defects of projections and computation of at least one point in each connected component of a real algebraic set*, Discrete Comput. Geom., 32 (2004), pp. 417–430.
[70] M. Safey El Din and É. Schost, *A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface*, Discrete & Computational Geometry, 45 (2011), pp. 181–220.
[71] M. Safey El Din and E. Schost, *A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets*, arXiv preprint arXiv:1307.7836, (2013).
[72] M. Safey El Din and L. Zhi, *Computing rational points in convex semialgebraic sets and sum of squares decompositions*, SIAM Journal on Optimization, 20 (2010), pp. 2876–2889.
[73] É. Schost, *Computing parametric geometric resolutions*, Applicable Algebra in Engineering, Communication and Computing, 13 (2003), pp. 349–393.
[74] M. Schweighofer, *Global optimization of polynomials using gradient tentacles and sums of squares*, SIAM Journal on Optimization, 17 (2006), pp. 920–942 (electronic).
[75] I. Shafarevich, *Basic Algebraic Geometry 1*, Springer Verlag, 1977.
[76] N. Z. Shor, *An approach to obtaining global extrema in polynomial problems of mathematical programming*, Kibernetika (Kiev), (1987), pp. 102–106, 136.
[77] P.-J. Spaenlehauer, *Complexity bounds for computing critical points with gr\" obner bases algorithms: the mixed case*, arXiv preprint arXiv:1309.2138, (2013).